
UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation) **Docket No. _______**
)

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

Lauren Perotti
Assistant General Counsel
Marisa Hecht
Senior Counsel
North American Electric Reliability
Corporation
1401 H Street NW, Suite 410
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

July 10, 2024

TABLE OF CONTENTS

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation) **Docket No. _______**
)

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA")[1] and Section 39.5 of the regulations of the Federal Energy Regulatory Commission ("FERC" or "Commission"),[2] the North American Electric Reliability Corporation ("NERC")[3] hereby submits for Commission approval the following eleven proposed Critical Infrastructure Protection ("CIP") Reliability Standards:[4]

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-10 - Cyber Security – Security Management Controls
- CIP-004-8 - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – Electronic Security Perimeter(s)
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-4 - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

---

[1] 16 U.S.C. § 824o.

[2] 18 C.F.R. § 39.5 (2023).

[3] The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006) *order on reh'g & compliance,* 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC,* 564 F.3d 1342 (D.C. Cir. 2009) [hereinafter ERO Certification Order].

[4] Unless otherwise indicated, all capitalized terms used in this petition shall have the meaning set forth in the Glossary of Terms used in NERC Reliability Standards ("NERC Glossary"), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

For the reasons discussed below, NERC requests that the Commission approve the proposed Reliability Standards, provided in **Exhibit A** hereto, as just, reasonable, not unduly discriminatory or preferential, and in the public interest. NERC also requests approval of: (1) four new and 18 proposed revised definitions, as shown in **Exhibit A**, for inclusion in the NERC Glossary; (2) the associated Implementation Plan (**Exhibit B**); (3) the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (**Exhibit F**); and (4) the retirement of currently effective Reliability Standards.[5]

As required by Section 39.5(a) of the Commission's regulations,[6] this petition presents the technical basis and purpose of the proposed Reliability Standards, a summary of the development history (**Exhibit G**), and a demonstration that the proposed Reliability Standards meet the criteria identified by the Commission in Order No. 672[7] (**Exhibit C**). The NERC Board of Trustees adopted the proposed Reliability Standards on May 9, 2024.

I. SUMMARY

Over the past decade, technology supporting and enabling the industrial control systems that operate the Bulk-Power System has evolved rapidly. Along with that evolution, the risks facing the Bulk Power System and the methods for mitigating those risks have also evolved. To accommodate this evolution, the NERC CIP Reliability Standards must provide Responsible Entities[8] the flexibility to adopt new and innovative technologies to operate their systems effectively and efficiently while maintaining a robust security posture.

---

[5] NERC is requesting the retirement of CIP-002-5.1.a, CIP-003-9, CIP-004-7, CIP-005-7, CIP-006-6, CIP-007-6, CIP-008-6, CIP-009-6, CIP-010-4, CIP-011-3, and CIP-013-2.

[6] 18 C.F.R. § 39.5(a).

[7] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC 61,104 at PP 262, 321-37 (2006) [hereinafter Order No. 672], *order on reh'g*, Order No. 672-A, 114 FERC 61,328 (2006).

[8] As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entity responsible for the implementation of and compliance with a particular requirement.

One such technological advance has been the proliferation of virtualization technologies. The National Institute of Standards and Technology ("NIST") defines virtualization as "the process of creating virtual, as opposed to physical, versions of computer hardware to minimize the amount of physical hardware resources required to perform various functions."[9] The proposed revisions to the CIP Reliability Standards and NERC Glossary are designed to support reliability by addressing the use of virtualization technologies in environments subject to the CIP Reliability Standards. The proposed standards provide Responsible Entities an opportunity to take advantage of the newer concepts and efficiencies facilitated by virtualization as well as implement innovative security techniques enhanced by virtualization. Under the proposed revisions, Responsible Entities may still maintain perimeter-based network security but may also choose to adopt different, but effective, security approaches, such as Zero Trust Architecture,[10] around communications with applicable systems.

The suite of cyber security CIP Reliability Standards is a framework that applies protections to BES Cyber Systems based on their impact to the Bulk Electric System ("BES") if rendered unavailable, degraded, or misused. This framework categorizing BES Cyber Systems into high, medium, and low impact was established in the "Version 5"[11] Reliability Standards

---

[9] *Virtualization and Cloud Computing Services, Notice of Inquiry*, 170 FERC ¶ 61,110 at P 4 (2020) (citing the National Institute of Standards and Technology, Guide to Security for Full Virtualization Technologies, Special Publication 800-125 (Jan. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf.)

[10] According to the NIST, Zero Trust Architecture is defined as "A security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The zero trust security model eliminates implicit trust in any one element, component, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses." NIST, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, Special Publication 800-160, Vol. 2, Rev. 1, App. A pg. 70 (Dec. 2021), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

[11] The "Version 5" Reliability Standards refer to CIP-002-5.1a, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1.

that became effective in the United States in 2016. During implementation, industry recognized opportunities for improvement to the standards, including addressing the use of virtualization.

As discussed below, the use of virtualization, which provides for the separation, or abstraction,[12] of the physical components from the software components (such as an operating system), is not specifically addressed within the currently enforceable CIP Reliability Standards framework. The current framework, adopted as part of the "Version 5" revisions, was designed around the concept that devices have a one-to-one relationship between software and hardware. Many of the required controls are thus designed to fit that concept. A fundamental element in the currently enforceable CIP Reliability Standards revolves around implementation of a "perimeter-based" security model, through the establishment of an Electronic Security Perimeter, to manage communications to BES Cyber Systems through an Electronic Access Point.

This approach, however, does not allow for Responsible Entities to take full advantage of the benefits of virtualization, including the adoption of other security models, such as Zero Trust Architecture, that are enhanced with virtual network technologies. For instance, with Zero Trust Architecture, Responsible Entities can manage communications in a granular, "no trust" manner to address threats that could exist inside traditional, perimeter-based models.

The proposed CIP Reliability Standards and associated definitions are thus designed to facilitate the use of the full range of virtualized technologies securely. The proposed Reliability Standards not only allow entities to more fully implement virtualization, but they also address the risks associated with virtualized environments, such as "side channel" attacks where virtual systems executing on the same hardware could affect one another. The proposed standards do so by leveraging "security objectives" to focus requirements on the essential elements a

---

[12] Abstraction in the virtualization context means the separation or isolation of software, such as operating systems, and other data from the underlying hardware.

Responsible Entity must meet to support reliability. The use of security objectives establishes a framework that could adapt to newer technologies and innovative security models. Recognizing that virtualization technologies will not be adopted uniformly across all Responsible Entities or across all Responsible Entity environments, the proposed CIP Reliability Standards would permit Responsible Entities with more "traditional" architecture to continue with their current configurations.

The most significant changes in the proposed Reliability Standards occur to the "technical" CIP Reliability Standards (i.e., those standards focused on technical as opposed to administrative or procedural controls) and their associated definitions: proposed Reliability Standard CIP-005-8 – Cyber Security – Electronic Security Perimeter(s), proposed Reliability Standard CIP-007-7 – Cyber Security – Systems Security Management, and proposed Reliability Standard CIP-010-5 – Cyber Security – Configuration Change Management and Vulnerability Assessments. These changes addressing virtualization fall into four general categories:

1. Support of different security models by adjusting language around perimeter-based models to accommodate other security models, where more granular, policy-based controls may be used;
2. Recognition of virtualization infrastructure and virtual machines through new and revised terms in the NERC Glossary;
3. Broadening of change management approaches beyond a baseline-only configuration to recognize the dynamic nature of virtualized technologies, such as container technology[13] where applications are "virtualized" and no longer installed on specific servers; and
4. Managing accessibility and attack surfaces of a virtualized configuration.

---

[13] *See* Section IV.A.1 of this petition for background on some key concepts of virtualized technologies.

Each of these changes was considered in the context of the CIP framework and incorporated to support the current security posture of Responsible Entities and to allow for enhanced security posture when using other, newer technologies.

In addition to addressing virtualization, the proposed Reliability Standards support reliability by clarifying concepts that NERC, the Regional Entities, and Responsible Entities identified during implementation of prior versions of the CIP Reliability Standards, including Interactive Remote Access, CIP Exceptional Circumstances, and Technical Feasibility Exceptions.[14]

NERC requests that the Commission approve the proposed Reliability Standards and associated definitions as just, reasonable, not unduly discriminatory or preferential, and in the public interest. The proposed Reliability Standards enhance reliability with security objectives that help transform the CIP Reliability Standards into a framework that can support cyber security of the grid now and into the future.

---

[14] Technical Feasibility Exceptions are defined in Appendix 2 to the NERC Rules of Procedure, https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix%202%20eff%2020240627_signed.pdf.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[15]

Lauren Perotti Assistant General Counsel Marisa Hecht Senior Counsel North American Electric Reliability Corporation 1401 H Street NW, Suite 410 Washington, D.C. 20005 202-400-3000 Marisa.hecht@nerc.net Lauren.perotti@nerc.net	Soo Jin Kim Vice President and Director of Engineering and Standards North American Electric Reliability Corporation 3353 Peachtree Road, N.E. Suite 600, North Tower Atlanta, GA 30326 404-446-2560 Soo.jin.kim@nerc.net

III. BACKGROUND

The following background information is provided below: (a) an explanation of the regulatory framework for NERC; (b) a description of the NERC Reliability Standards Development Procedure; and (c) the history of Project 2016-02.

A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[16] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Bulk-Power System, and with the duty of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1) of the FPA states that all users, owners, and operators of the Bulk-Power System in the United States will be subject to Commission-approved Reliability Standards.[17] Section 215(d)(5) of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard.[18]

---

[15] NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203, to allow the inclusion of more than two persons on the service list in this proceeding.

[16] 16 U.S.C. § 824o.

[17] *Id.* § 824(b)(1).

[18] *Id.* § 824o(d)(5).

Section 39.5(a) of the Commission's regulations requires the ERO to file for Commission approval each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to make effective.[19]

The Commission has the regulatory responsibility to approve Reliability Standards that protect the reliability of the Bulk-Power System and to ensure that such Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Pursuant to Section 215(d)(2) of the FPA and Section 39.5(c) of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard.[20]

B. NERC Reliability Standards Development Procedure

The proposed Reliability Standards were developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[21] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[22] In its ERO Certification Order, the Commission found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain criteria for approving Reliability Standards.[23] The development process is open to any person or entity with a legitimate interest in the reliability of the Bulk-Power System. NERC considers the comments of all stakeholders.

---

[19] 18 C.F.R. § 39.5(a).

[20] 16 U.S.C. § 824o(d)(2); 18 C.F.R. § 39.5(c)(1).

[21] Order No. 672 at P 334.

[22] The NERC Rules of Procedure are available at https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx. The NERC Standard Processes Manual is available at https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix_3A_SPM_Clean_Mar2019.pdf.

[23] ERO Certification Order at P 250.

Further, a vote of stakeholders and adoption by the NERC Board of Trustees is required before NERC submits the Reliability Standard to the Commission for approval.

C. Development of the Proposed Reliability Standards

As further described in **Exhibit G** hereto, NERC initiated standard development Project 2016-02 Modifications to CIP Standards ("Project 2016-02") to address the directives from Order No. 822[24] as well as issues identified during implementation of the CIP Reliability Standards approved in Order No. 791.[25] Given the highly technical nature of the proposed revisions and the need to respond to Responsible Entities' comments for maintaining perimeter-based controls while also allowing for different security models, the Project 2016-02 drafting team dedicated several ballot periods to developing the language that achieved consensus: one initial comment period and ballot, and four additional comment periods and ballots. In addition, the Project 2016-02 drafting team completed several other items on its SARs, such as addressing FERC directives from Order No. 822 regarding protection of transient electronic devices, protections for communications network components between Control Centers, and revising electronic access controls for low impact BES Cyber Systems, among others, prior to focusing on virtualization. The first draft of the proposed standards were posted for an initial 60-day formal comment period and ballot from January 22 – March 22, 2021.

As the Reliability Standards achieved consensus during different additional ballot periods, the following tables provide the approval percentage for those Reliability Standards that passed in the third and fourth additional ballots.[26] The final ballot percentage approvals are

---

[24] *Revised Critical Infrastructure Protection Reliability Standards*, 154 FERC ¶ 61,037, Order No. 822 at PP 32, 73, *reh'g denied*, Order No. 822-A, 156 FERC ¶ 61,052 (2016).

[25] *Version 5 Critical Infrastructure Protection Reliability Standards*, 145 FERC ¶ 61,160, Order 791 (2013) [hereinafter Order No. 791], *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

[26] Results from all ballots conducted as well as results of non-binding polls are provided in **Exhibit G**.

included in a separate table. The proposed new and revised definitions and the Implementation Plan associated with the Reliability Standards were included in the following ballots but not as a separate ballot pool.

The following Reliability Standards received the requisite approval during the third additional ballot from August 17 – October 7, 2022:

Standard	Approval	Quorum
CIP-002-7	94.63	77.89
CIP-006-7	92.60	78.07
CIP-008-7	95.67	77.74
CIP-009-7	95.38	77.74
CIP-011-4	82.59	77.74
CIP-013-3	82.88	77.74

The following Reliability Standards received the requisite approval during the fourth additional ballot from October 3 – November 29, 2023:

Standard	Approval	Quorum
CIP-003-10	93.80	82.94
CIP-004-8	84.73	84.41
CIP-005-8	72.73	84.41
CIP-007-7	89.32	84.41
CIP-010-5	74.46	84.75

The final ballot was conducted from April 3 – April 12, 2024, with the following final ballot results:

Standard	Approval	Quorum
CIP-002-7	94.37	84.62
CIP-003-10	93.63	85.86
CIP-004-8	86.3	86.1
CIP-005-8	75.73	86.1
CIP-006-7	94.7	83.84
CIP-007-7	90.24	86.1
CIP-008-7	96.05	83.84
CIP-009-7	95.8	83.84
CIP-010-5	76.98	86.44
CIP-011-4	86.21	83.84
CIP-013-3	86.47	83.84

As noted previously, the Board adopted the Reliability Standards and associated definitions on May 9, 2024.

IV. JUSTIFICATION FOR APPROVAL

NERC submits for Commission approval 11 proposed cyber security CIP Reliability Standards and four new and 18 revised defined terms used in the proposed standards for inclusion in the NERC Glossary. The proposed standards and definitions improve upon the current standards and definitions by further refining the standards' focus on security through the (1) use of objectives to permit use of a broader variety of security controls, (2) revision of requirements that focused more on compliance documentation, and (3) clarification of issues identified during implementation of prior versions of CIP Reliability Standards. As discussed below and in **Exhibit C**, the proposed Reliability Standards were developed in a fair manner and are just, reasonable, not unduly discriminatory or preferential, and in the public interest.

As noted above, there are four basic categories of the revisions in the proposed Reliability Standards: (1) addressing use of virtualization; (2) clarity on Interactive Remote Access; (3) additions to the application of CIP Exceptional Circumstances; and (4) revisions to Technical Feasibility Exception language. This section provides justification for each of these categories of revisions and then provides additional detail on the revisions within each of the standards and definitions.

Accordingly, Section IV is organized as follows: Sections IV.A-D provide high level overviews of the categories of proposed revisions, and Section IV.E provides more detail on the revisions and explains how those categories are incorporated into each standard and definition. Section IV.F provides an overview of other administrative, minor, conforming, or clarifying changes within the proposed CIP Reliability Standards. Section IV.G addresses the enforceability of the proposed Reliability Standards.

A. Addressing Use of Virtualization

As discussed above, the most significant revisions proposed herein are designed to better facilitate use of virtualization under the CIP Reliability Standards. The proposed Reliability Standards leverage security objectives, which not only facilitate use of virtualization but also further support adoption of evolving technology to help ensure resilient operation of industrial control systems.

Section IV.A provides background on the need for the revisions addressing virtualization as well as the justification for how these revisions accommodate certain aspects of virtualization. Section IV.A.1 provides background on virtualization concepts that can help to understand the infrastructure design. Section IV.A.2 describes the need for the proposed revisions to address these virtualization concepts within the CIP requirements. Finally, Section IV.A.3 provides a high-level overview of the revisions addressing virtualization throughout the suite of cyber security CIP Reliability Standards. Within Section IV.A.3, the justification for the proposed revisions is divided into the following subcategories: (1) support of different security models; (2) recognition of virtualization infrastructure and virtual machines characteristics; (3) broadening of change management approaches; and (4) managing accessibility and attack surfaces of a virtualized configuration.

1. Background on Virtualization Concepts

As noted previously, virtualization is "the process of creating virtual, as opposed to physical, versions of computer hardware to minimize the amount of physical hardware resources required to perform various functions."[27] There are several concepts behind virtualized

---

[27] *Virtualization and Cloud Computing Services, Notice of Inquiry*, 170 FERC ¶ 61,110 at P 4 (2020) (citing the National Institute of Standards and Technology, *Guide to Security for Full Virtualization Technologies,* Special Publication 800-125 (Jan. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf.).

environments that factored into the proposed revisions. This section provides high-level descriptions of some of the concepts most relevant to understanding the proposed Reliability Standards and definitions.

a. Shared Resources

A core tenet of virtualization is the ability to share hardware (both physical and virtualized), central processing units, memory, storage, and other resources among various virtualized operating systems, called "guest operating systems." The use of virtualization abstracts the software layers from the underlying hardware infrastructure so that it may be shared. Then, in some configurations, a hypervisor manages the interactions between shared resources and guest operating systems, helping to ensure isolation and control access, as appropriate. Depending on the form of virtualization, hypervisors run directly on the hardware (known as bare metal or native virtualization) or on a "host operating system" (known as hosted virtualization).[28] In other configurations, a container engine abstracts applications from the host operating system.

b. Virtual Machines

A virtual machine is a computing stack inside a virtualized host that consists of the guest operating system, one or more application programs, and at times, middleware.[29] Virtual machines can be created and destroyed dynamically and are neither always running nor tied to specific hardware. A "dormant" virtual machine is not currently executing or instantiated (i.e.,

---

[28] National Institute of Technology ("NIST"), *Guide to Security for Full Virtualization Technologies*, Special Publication 800-125 (Jan. 2011) at pg. 2-2, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf.

[29] NIST, *Secure Virtual Network Configuration for Virtual Machine (VM) Protection*, Special Publication 800-125B (Mar. 2016) at pg. 1, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125B.pdf. Middleware is "software that lies between an operating system and the applications running on it…middleware enables communication and data management for distributed applications." Microsoft, *What is middleware?* https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-middleware (last visited Jul. 8, 2024).

"booted up"). Dormant virtual machines exist as a file and may be dormant for a long period of time. Whereas "traditional" Cyber Assets on a network would be patched and updated on a regular basis, virtual machines are managed such that they would be updated as soon as they begin to instantiate after being in a dormant state. A virtual machine instantiates ("boots") from a disk image file. Since the boot "disk" is a file and not a physical disk, many individual virtual machines can use the same "parent" image as the basis for their own "child" image. Among other things, this allows for patching of an operating system to occur to a parent image, and the child images incorporate that patched image upon their next instantiation. A common use of parent and child images is virtual desktop infrastructure that delivers a temporary desktop environment to each remote user for the duration of a session that are virtual machines instantiated from a parent image.

c. Containers

Also called "application containers," containers are a form of virtualization at an individual application level, bundling the application code and its runtime environment into a self-contained, sandboxed environment that is separate from infrastructure, including from the host operating system. The application can then be instantiated dynamically on one or multiple dynamic hosts. The benefit is it makes the application or logic as portable as possible and able to be instantiated as-is without modification on a developer's workstation, a test environment, or a production data center without the notion of installing the application or the various runtime dependencies into a particular operating system instance.

2. Need for Proposed Virtualization Revisions

The following section provides detail on the need for the proposed revisions related to virtualization and is organized as follows: Section IV.A.2.a provides background information on the recommendations for revisions resulting from lessons learned during implementation of

Version 5 standards and discusses the benefits of virtualization; Section IV.A.2.b describes the security models that are facilitated by virtualization; and Section IV.A.2.c discusses how the proposed revisions help to ensure that the CIP Reliability Standards continue to accommodate future technologies.

a. Recommendations for Revisions Based on Version 5 Implementation

During implementation of the "Version 5" CIP Reliability Standards, NERC and the Regional Entities collaborated with industry stakeholders to help ensure a smooth transition to the revised framework of CIP Reliability Standards. This effort was in response to the Version 5 CIP Reliability Standards' shift in the way Responsible Entities classified BES Cyber Systems as low, medium, and high impact from previous versions of cyber security Reliability Standards. As a result, NERC, the Regional Entities, and industry stakeholders had the opportunity to assess potential issues with implementation of the Version 5 standards to consider whether further revisions were needed.[30] Among other things, this effort identified that the Version 5 CIP Reliability Standards did not specifically address use of virtualization. Accordingly, with the increasing use of virtualization in industrial control system environments, a drafting team needed to consider revisions to the CIP Reliability Standards that would clarify the permitted architecture and address the security risks of virtualization technologies.

While the effort during implementation of the Version 5 Reliability Standards identified an opportunity for revisions to address virtualization, NERC, the Regional Entities, industry stakeholders, and FERC recognized that virtualization could have benefits for Responsible Entities.

---

[30] NERC, *CIP V5 Issues for Standard Drafting Team Consideration* (Sept. 15, 2015), https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/Transfer_Issues_V5TAG-SDT_1st-final-03232016.pdf.

As discussed in the Project 2016-02 drafting team's white paper entitled "Virtualization and Future Technologies Project 2016-02 Standards Drafting Team: The Case for Change" (**Exhibit D**), the Project 2016-02 drafting team highlighted the following reliability benefits of virtualization:

- Virtualization facilitates increased uptime, fast recovery capability, and flexible architecture that can instantly adapt to changing workloads;
- Virtualization allows for racks of central processing units, memory, and disks to be considered "raw" computing resources within high speed mesh networks;
- If the workload on a particular virtual server is nearing capacity, the infrastructure orchestration system can create and configure an additional server on demand, bring it online to help with the peak workload, and then destroy it when it is no longer needed;
- If a physical machine runs out of resources, the workload can be moved to another physical machine dynamically based upon relative load. When a virtual server or workstation is not in use, it is similar to a physical server that is powered off;
- This flexible and dynamic architecture also allows Responsible Entities to leverage security controls such as those provided by micro-segmentation; and
- Users can be granted access to specific workloads that can be placed dynamically throughout the infrastructure with managed access to provided services.

Similarly, public commenters provided input on the benefits of virtualization in a Commission proceeding in Docket No. RM20-8-000. In a Notice of Inquiry, the Commission sought comment regarding the potential benefits and risks associated with the use of virtualization and cloud computing services in association with Bulk Electric System operations.[31] In response, commenters provided the following benefits of virtualization:

- Faster recovery of systems;
- Faster and more standardized deployment of systems and maintenance;
- Flexibility of resource allocation;
- Scalability of environment and potential cost savings;
- Ability to use products only supported by a virtualized environments;
- Reduced dependency on older hardware; and
- Allows for the pooling of excess hardware capacity for meeting peak workloads.[32]

Based on comments received, the Commission recognized that the commenters generally agreed that virtualization can bring significant benefits as long as risks are mitigated.[33] In addition, the Commission noted it supported NERC's efforts to assess the CIP Reliability Standards to facilitate adoption of virtualization and complete Project 2016-02, noting that virtualization should continue to be voluntary for entities.[34] As described below, the Project 2016-02 drafting team determined that any revisions to the CIP Reliability Standards must permit Responsible Entities the opportunity to take advantage of the benefits of advanced virtualization features while also preserving their choice to maintain current secure perimeter-based network architecture, which continues to be a valid network security model.

---

[31] *Virtualization and Cloud Computing Services*, Notice of Inquiry, 170 FERC ¶ 61,110 (2020).

[32] Comments were submitted in FERC docket number RM20-8-000.

[33] *Virtualization and Cloud Computing Services*, Order Directing Informational Filing, 173 FERC ¶ 61,243, at P 2 (2020).

[34] *Id.* at PP 14-15.

b. Virtualization and Security Models

As mentioned above, with the benefits of virtualization, Responsible Entities also need effective security models to mitigate any risks. While Responsible Entities can deploy the perimeter-based network security model to virtualization, other security models are available and allow access controls at a much deeper level within the infrastructure. One such model is Zero Trust Architecture. According to NIST, Zero Trust Architecture is "[a] security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The [zero-trust] security model eliminates implicit trust in any one element, component, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses."[35] As described in this section, Zero Trust Architecture has been supported by the White House in dictating how the federal government should approach cyber security as well as the Commission in other proceedings.

In 2021, President Biden issued an Executive Order on improving the nation's cybersecurity.[36] One aspect of the Executive Order directed the federal government to "advance toward Zero Trust Architecture" as part of modernizing federal government cyber security.[37] To carry out the Executive Order, the White House issued a memorandum outlining a zero trust

---

[35] NIST, *Computer Security Resource Center Glossary*, https://csrc.nist.gov/glossary/term/zero_trust_architecture.

[36] Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 12, 2021), https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

[37] *Id.* at 26,635.

strategy for federal government, noting that "[a] transition to a 'zero trust' approach to security provides a defensible architecture for this new [threat] environment."[38]

Furthermore, the Commission itself has encouraged use of zero trust principles in the CIP Reliability Standards. In Order No. 887, the Commission directed NERC to develop requirements for internal network security monitoring for all high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity, stating that internal network security monitoring is a "fundamental element of a zero-trust architecture."[39] Based on the focus of the federal government on advancing Zero Trust Architecture as a security model, it follows that NERC should ensure that its CIP Reliability Standards do not prevent entities from adopting this security model.

c. Forward-looking

The proposed revisions are also needed to help ensure the CIP Reliability Standards are forward-looking and continue to allow Responsible Entities to adopt different security models as emerging risks evolve. Specifically, the proposed revisions accomplish this through security objectives. Many of the basic concepts of the CIP framework are essentially unchanged from the Urgent Action 1200 standard in 2003. The primary focus of those standards was the "critical cyber asset," an "electronic device" such as a server, workstation, or relay as a physical object. It had an operating system, always on and performing its function, and communicating with other components over routable protocols. It was protected by traditional firewalls at the network edge

---

[38] The White House, Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, at p. 2 (Jan. 26, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[39] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021, at P 32 (2023) (referencing *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems* Notice of Proposed Rulemaking, 178 FERC ¶ 61,038, at P 30 (2022)).

looking at source and destination protocol addresses and ports as the only mechanism by which to make network access control decisions.

Today, newer technology has changed this scenario. With virtualization, physical devices are no longer the primary units of organization. An entire control system infrastructure can be virtualized (such as “software defined data centers”) and only exist as logical constructs. An energy management system database server may never exist as a discrete physical object. With containers, there may not be a concrete tie between application logic and an operating system. Virtual machines can be created and destroyed dynamically and are neither always on, nor tied to specific hardware. Workloads may mirror their information for reliability purposes across great distances without using routable protocols. With microsegmentation, network access control lists are now much more granular than internet protocol addresses at a perimeter. They are enhanced by policy-based control templates enforcing access at a “user to workload” level throughout the system infrastructure. Electronic access control may no longer be based solely on routable protocol addresses or found only at an Electronic Security Perimeter boundary.

In addition to virtualization, there are other technologies on the horizon that may become commonly used for industrial control systems. The Commission itself has recognized that, “[v]irtualization is a necessary technical enabler if the functions of BES Cyber Systems are to be moved to a cloud computing environment since a customer choosing to migrate one or more on-premise systems to the cloud will need to virtualize those systems for use in the cloud.”[40] Cloud services already permeate several aspects of the corporate side of utility businesses, as well as storage of BES Cyber System Information. In the same Notice of Inquiry into virtualization benefits and risks, the Commission solicited comment on performing BES operations in the

---

[40] *Virtualization and Cloud Computing Services*, Notice of Inquiry, 170 FERC ¶ 61,110, at P 6 (2020).

cloud. Moreover, the Commission directed NERC to initiate a study of BES operations in the cloud.[41] Based on that study, there is a Standard Authorization Request looking into revisions to the CIP Reliability Standards regarding use of cloud.[42] While virtualization and cloud services are different, the use of security objectives in the proposed revisions help to advance the CIP Reliability Standards toward maintaining relevance in light of changing technologies.

3. Overview of Proposed Revisions Addressing Virtualization

As noted above, there are unique characteristics and benefits of virtualization that are addressed in the proposed CIP Reliability Standards revisions. This section provides an overview of the proposed revisions addressing virtualization that fall into the following four general categories: (a) support of different security models; (b) recognition of virtualization infrastructure and virtual machines characteristics; (c) broadening of configuration change management approaches; and (d) managing accessibility and attack surfaces of virtualized configurations.

a. Support of Different Security Models

As discussed in Section IV.A.2.b of this petition, one of the driving needs for revisions to the CIP Reliability Standards was to accommodate different security models. In particular, the requirement in CIP-005-7 to implement a perimeter-based network security model limited Responsible Entities to a single security model. As such, the Project 2016-02 drafting team developed revisions to Requirements R1 and R2 in CIP-005-8 (more fully detailed in Section IV.E.5 of this petition) to focus on the security objective of securing communications to and

---

[41] NERC completed the study through collaboration with the NERC Security Integration and Technology Enablement Subcommittee ("SITES"), a subgroup of the NERC Reliability and Security Technical Committee. NERC SITES, *BES Operations in the Cloud*, White Paper (Sept. 2023), https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SITES_WhitePaper_BES_Ops_in_Cloud.pdf

[42] NERC, *Project 2023-09 Risk Management for Third-Party Cloud Services*, https://www.nerc.com/pa/Stand/Pages/Project-2023-09-Risk-Management-for-Third-Party-Cloud-Services.aspx.

from BES Cyber Systems. In addition, the proposed revisions permit Responsible Entities to either continue with the perimeter-model configuration or leverage more granular, policy-based controls facilitated by virtualized environments. Throughout the CIP Reliability Standards, the Project 2016-02 drafting team updated language to remove concepts such as “inside” an Electronic Security Perimeter and replaced that with more inclusive phrases such as “protected by” an Electronic Security Perimeter in recognition of security models that may have policy enforcement points controlling access to BES Cyber Systems rather than a “perimeter.”

In conjunction with the revisions in CIP-005-8, the drafting team revised the definitions of Electronic Security Perimeter, Electronic Access Point, and External Routable Connectivity to further support adoption of other security models (more fully described in Section IV.E.1 of this petition).

b. Recognition of Virtualization Infrastructure and Virtual Machines Characteristics

At their inception, the current suite of CIP Reliability Standards did not contemplate virtual machines, application containers, and other virtualized infrastructure. As such, Responsible Entities face challenges in applying the requirements to virtualized infrastructure. The proposed revisions to the Reliability Standards and definitions recognize the unique characteristics of virtual infrastructure and address how hardware relates to the software and data.

For example, the NERC Glossary term Cyber Assets is defined as “programmable electronic devices, including the hardware, software, and data in those devices.” As this definition includes hardware components for each device, it does not account for devices in virtualized environments that share hardware resources. The Cyber Asset definition assumes a one-to-one relationship between a device, such as a BES Cyber Asset, and its hardware. Virtualization, however, changes that relationship to a "one-to-many" because in some cases, hundreds of virtual BES Cyber Assets can share a pool of hardware resources (compute, network, and storage resources). As such, the Project 2016-02 drafting team sought to develop revisions to the suite of CIP Reliability Standards that recognize the following three asset classes that exist with the introduction of virtualized technologies in industrial control systems:

- Self-contained devices that are composed of dedicated hardware, some form of operating system or firmware, and the application code. This is the traditional definition of a Cyber Asset and applies to things such as digital relays, remote terminal units, physical operator workstations, and dedicated physical servers.
- Virtual "cyber assets" composed of an operating system and applications or containers minus any dedicated hardware. These types of assets are logical or virtual constructs by nature and exist only in memory or files. They can, however, appear from a network perspective the same as any other host.
- Shared infrastructure consists of the hardware resource pools (compute, network, and storage) and is shared by virtual cyber assets and can host numerous virtual cyber assets, networks, or storage locations.

In addition to recognizing the different asset classes listed above, the revisions that fall under this category recognize that the proposed requirements must address controlling access and communications to the management plane of shared infrastructure. Access to the management plane (also known as the interface or console) permits users to create, modify, or delete virtualized objects (such as servers, networks, switches, firewalls, or storage) or even entire virtualized infrastructure. Moreover, access to the management plane permits users to move virtualized objects from one security zone to another.

In recognition of the characteristics of virtual machines and their underlying infrastructure, the proposed revised requirements and new and revised definitions apply protections where they are needed rather than relying on the one-to-one relationship between hardware and software in the currently defined Cyber Assets. As a result, the proposed requirements permit Responsible Entities to use protections that are appropriate and secure for virtualization. The proposed revisions help to address risks, for example, by preventing use of "mixed trust" environments where virtual machines of varying impact levels share the same central processing units, among other components, and the occurrence of "side channel" attacks where virtual systems executing on the same hardware could affect one another. Moreover, the proposed requirements include appropriate protections for the management plane to secure access. The following proposed definitions and revisions account for the characteristics of virtual machines and underlying infrastructure:

- Cyber Asset and Virtual Cyber Asset definitions (see Section IV.E.1)
- Shared Cyber Infrastructure development (see Section IV.E.1)
- Management Interface development (See Section IV.E.1)
- Cyber Systems (See Section IV.E.1)

c. Broadening of Configuration Change Management Approaches

The proposed Reliability Standards broaden configuration change management approaches to reflect certain characteristics of the technologies enabled by virtualization. According to NIST, configuration management is "[a] collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle."[43]

As part of that management, Responsible Entities need to control for configuration changes to help ensure that neither adverse impacts nor unauthorized changes occur. In the virtualization context, there are several unique characteristics, such as shared infrastructure, remediation Virtual Local Area Network,[44] containers, parent and child images, and dormant virtual machines that require a broader approach to configuration change management than currently exists in the CIP Reliability Standards. For instance, the dynamic management of application containers, with the ability to instantiate the application on the best "node" (e.g., server) at the moment, renders the current CIP Reliability Standards more of a documentation exercise of that dynamic management rather than a true focus on the security of changes made in a virtualized environment.

As such, the proposed revisions in Reliability Standard CIP-010-5 focus on a security objective of controlling the implementation of intended changes to software or settings that could weaken certain cyber security controls rather than only software items listed in a baseline configuration. Moreover, the focus of change management around the technical controls in CIP-005 and CIP-007, with comprehensive evaluation and testing of the potential impacts to those controls, should provide Responsible Entities with an accurate picture of the current and future

---

[43] NIST, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53 rev. 5, at App. A pg. 398 (Dec. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[44] NIST defines Local Area Network as "a group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network." NIST, *Mobile Device Security: Corporate-Owned Personally-Enabled*, Special Publication 1800-21 at App. B at p. 165 (Sep. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-21.pdf. A remediation Virtual Local Network is a network segment in which a Cyber Asset or Virtual Cyber Asset is placed so that its security posture can be evaluated before joining its intended network. Upon passing the configured policy checks or being remediated such that it passes, it is then allowed to connect to or communicate on its intended network.

state of the Cyber System. In so doing, the proposed revisions provide Responsible Entities the opportunity to focus more on a forward-looking authorization of a change rather than a backward-looking baseline update for compliance purposes. These proposed changes are further described in detail in Section IV.E.10 below.

d. Managing Accessibility and Attack Surfaces of a Virtualized Configuration

As mentioned above, the characteristics of virtualized environments require an updated approach to managing accessibility and reducing the attack surface of a virtualized configuration. With the introduction of shared resources, hardware-based vulnerabilities need to be addressed differently to mitigate compromise across processes simultaneously executing on the same hardware and across impact categorizations. For example, securing the accessibility of the physical underlay of the shared infrastructure may be better facilitated by managing at the service level versus the port numbers.

Accordingly, the Project 2016-02 drafting team proposed revisions in CIP-007 to manage system security and accessibility. For instance, current CIP-007-6, Requirement R1 focuses on ports and services and the disabling or restricting of those unneeded ports or services. However, in Zero Trust Architecture, for example, accessibility may be gained through a "user to tagged workload" level access control policy instead of an enabled port or service. As a result, the revisions in proposed CIP-007-7, Requirement R1 focus on the security objective of disabling or preventing unneeded routable protocol network accessibility to account for more varied security controls in the future. Proposed changes in CIP-007-7 are discussed in more detail in Section IV.E.7 below.

B. Interactive Remote Access

The Project 2016-02 drafting team considered clarification to the use of Interactive Remote Access based on feedback obtained during implementation of the "Version 5" CIP Reliability Standards. These proposed revisions to CIP-005 and the Interactive Remote Access definition support reliability by clarifying when certain non-routable (serial) Cyber Systems should be subject to the CIP-005 requirements for Interactive Remote Access on the routable portion of the remote access connection. In particular, the drafting team addressed the risk of those Cyber Systems that are serial, non-routable devices but are "reachable" through the availability of Interactive Remote Access. Because these Cyber Systems are not directly connected to a network with a routable protocol, it was unclear if they had an "associated Electronic Security Perimeter" that resulted in External Routable Connectivity upon which Interactive Remote Access depended. Thus, some of the proposed revisions remove those dependencies and clarify that CIP-005 requirements will apply if: (1) a medium or high impact BES Cyber System only has non-routable connectivity (i.e., serial) but is subsequently converted to routable protocol; and (2) a remote user can still gain Interactive Remote Access to the BES Cyber System.

C. CIP Exceptional Circumstances

Within the CIP Reliability Standards, certain requirements include an exception for instances that meet the definition of CIP Exceptional Circumstances,[45] which entities may declare during certain, defined emergencies to temporarily suspend complying with specific CIP

---

[45] The NERC Glossary defines a CIP Exceptional Circumstance as, "[a] situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability."

standards requirements in the interest of supporting reliability. Reliability Standard CIP-003 requires Responsible Entities develop a policy for how to declare and respond to CIP Exceptional Circumstances. Often, these exceptions are attached to requirements that may be more documentation-oriented or compliance-oriented. These exceptions support the reliability of the Bulk Power System by permitting Responsible Entities to focus more on security and reliability than on compliance-related activities in certain discrete circumstances.

During implementation of Version 5, Responsible Entities recognized other requirements that may be appropriate for declaring a CIP Exceptional Circumstance as needed. The Project 2016-02 drafting team reviewed all requirements to determine those that should allow exceptions during CIP Exceptional Circumstances. Based on this review, the following proposed requirements include new exceptions during CIP Exceptional Circumstances or were moved within the requirements:

- CIP-004-8, Requirement R3, Part 3.5;
- CIP-006-7, Requirement R2 (Previously, Parts 2.1 and 2.2 had CIP Exceptional Circumstances. Including the CIP Exceptional Circumstances in the parent requirement now extends its applicability to Part 2.3 as well); and
- CIP-010-5, Requirement R1, Part 1.2.1 (previously was Part 1.5).

D. Technical Feasibility Exceptions

Several of the proposed revisions fall under the category of removing language triggering Technical Feasibility Exceptions and replacing it with “per system capability.” As background, in Order No. 706, FERC approved eight CIP Reliability Standards and, among other things, directed NERC to develop a set of conditions or criteria that a registered entity must follow to obtain a Technical Feasibility Exception from specific requirements in the CIP Reliability

Standards.[46] In response to this directive and subsequent directives on further refinements,[47] NERC developed Appendix 4D of the NERC Rules of Procedure that governs the process for requesting and receiving Technical Feasibility Exceptions. With the transition to the CIP Version 5 Reliability Standards, NERC and the Regional Entities observed a significant decrease in the number of Technical Feasibility Exceptions.[48] This decrease has enabled the Regional Entities to better evaluate the risk and impact of Technical Feasibility Exceptions and gain a more complete understanding of the value of the Technical Feasibility Exceptions process compared to the administrative burden it places on Responsible Entities and Regional Entities. As a result, the Project 2016-02 drafting team took the opportunity to evaluate and eliminate the use of requirement language triggering Technical Feasibility Exceptions.

Instead, the proposed revisions use the term "per system capability" to account for the different types of technology that will be expected to meet the security objective. With the use of this language, Responsible Entities will continue to be responsible for implementing an equally effective method, if necessary and capable, to meet the ultimate security objective for each

---

[46] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040 at P 178 (2008) [hereinafter Order No. 706], *order on clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009), *order deny'g request for clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

[47] *N. Am. Elec. Reliability Corp.*, 130 FERC ¶ 61,050 (2010) [hereinafter January 21 Order], *order on compliance*, 133 FERC ¶ 61,008 (2010) [hereinafter October 1 Order], *order on reh'g*, 133 FERC ¶ 61,209 (2010), *order on compliance*, 135 FERC ¶ 61,026 (2011) [hereinafter April 12 Order].

The Commission requested further information and clarification regarding certain aspects of the TFE process. On April 21, 2010, NERC submitted its compliance filing in response to the January 21 Order. On October 1, 2010, the Commission issued an order accepting NERC's April 2010 filing as partially compliant and directing further changes to the TFE Procedure. *See* October 1 Order. On December 23, 2010, NERC submitted a compliance filing in response to the Commission's October 1 Order, which the Commission subsequently accepted. *See* April 12 Order; *see also N. Am. Elec. Reliability Corp.*, 144 FERC ¶ 61,180 at PP 14, 17-18 (2013) [hereinafter September 2013 Order]; *see also N. Am. Elec. Reliability Corp.*, Docket No. RR13-3-001 (Jan. 30, 2014) (delegated letter order).

[48] NERC reports on these observations in its Annual Reports on Wide-Area Analysis of Technical Feasibility Exceptions in FERC Dockets Nos. RR10-1-000 and RR13-3-000.

requirement where this language appears. The use of the phrase "per system capability" is further described in Section IV.E regarding certain instances within the proposed requirements.

E. Standards and Definitions

Section IV.E discusses the proposed revisions to each Reliability Standard and NERC Glossary definitions in more detail, with a particular focus on the revisions in the proposed "technical" Reliability Standards CIP-005-8, CIP-007-7, and CIP-010-5.

1. Definitions

There are 18 proposed revised terms used in the NERC *Glossary* and four new proposed terms, which include Cyber System, Management Interface, Shared Cyber Infrastructure, and Virtual Cyber Asset (clean and redline definitions provided in **Exhibit A-12**). In developing these terms, the drafting team focused on keeping the terms more definitional than scoping mechanisms, moving any "requirement-type" language to actual requirements for greater clarity. The following section provides detail around some of the more significant changes within the definitions. Additional explanation of all the proposed revised and new definitions are included in the technical rationale document, **Exhibit E-12** hereto.[49]

Cyber Asset

As mentioned above, the current Cyber Asset definition assumes a one-to-one relationship between software and physical hardware. As such, the drafting team proposed modifications to the Cyber Asset definition to explicitly exclude Shared Cyber Infrastructure because it is a different hardware class on which the other Virtual Cyber Assets of differing impact levels execute. This separation also allows Shared Cyber Infrastructure to be added to

---

[49] Those definitions not described in this section below were more minor or conforming changes, including adding in Shared Cyber Infrastructure, Management Interface, or Virtual Cyber Asset where appropriate; changing "Cyber Asset" to "Cyber System"; revising references to Electronic Security Perimeters; or replacing terms with their acronyms, and can be found in **Exhibit A-12** with further technical rationale provided in **Exhibit E-12**.

applicability based on its unique risks. The revised definition also clarifies that "application containers" (i.e., portable, packaged applications) are considered software of a Cyber Asset (or Virtual Cyber Asset), though they may have some characteristics of a Virtual Cyber Asset (a container can be instantiated with its own internet protocol address, etc.). In addition, the Project 2016-02 drafting team developed the proposed Virtual Cyber Asset definition to distinguish it from the Cyber Asset definition, as described later in this section.

Cyber System

Cyber System is a proposed newly defined term that states: "One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure." This definition groups the three "asset classes" that are subject to the CIP Reliability Standards into one NERC Glossary term for readability so that CIP requirements typically mentioning "Cyber Assets" can now easily refer to Cyber Assets, Virtual Cyber Assets, and Shared Infrastructure in one term.

Electronic Access Control or Monitoring Systems (EACMS)

The proposed revisions to the definition of Electronic Access Control or Monitoring Systems ("EACMS"), shown in blackline, are as follows:

> Cyber ~~Assets~~ **System(s)** that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) **(ESP)** or BES Cyber Systems~~.~~ **(BCS), including those not protected by an ESP used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS** ~~This includes Intermediate Systems~~.

The proposed EACMS definition now includes "Cyber Systems" instead of Cyber Assets to demonstrate that EACMS can also take the form of Virtual Cyber Assets and Shared Cyber Infrastructure in addition to Cyber Assets. The reference to Intermediate System has been removed as the revisions to the definition of Intermediate System now directly reference

EACMS. Finally, the proposed EACMS definition includes language clarifying when a protocol converter (e.g., serial to routable) would be considered an EACMS.

Electronic Access Point

The proposed revisions to the definition of Electronic Access Point, shown in blackline, are as follows:

> ~~**A**~~ **An electronic policy enforcement point or a** Cyber Asset interface on an Electronic ~~**Security Perimeter**~~ **Access Control or Monitoring Systems** that ~~**allows**~~ **controls** routable communication ~~**between**~~ **to and from one or more BES Cyber Systems or their associated Protected** Cyber Assets ~~**outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter**~~.

As network security moves deeper into the infrastructure, it is no longer necessary to prescribe that network security be performed only at a "Cyber Asset interface on an Electronic Security Perimeter" at one point on a network edge. Zero Trust Architecture, for example, highly distributes the network security model and is not perimeter-based. This model is incorporated into the definition through the addition of "electronic policy enforcement point." With the added flexibility in CIP-005 to adopt these models in addition to the traditional perimeter-based model, the proposed modifications to the Electronic Access Point definition allow for the use of electronic policy enforcement points rather than prescribing a specific architecture. The "one or more" and the "associated Protected Cyber Assets" have been added to clarify that Electronic Access Points can control communications to a group and are not required per individual system.

External Routable Connectivity

The proposed revisions to the definition of External Routable Connectivity, shown in blackline, are as follows:

> The ability to access a BES Cyber System ~~**from a Cyber Asset that is outside of its associated**~~ **through its** Electronic Security Perimeter via a bi-directional routable protocol connection.

The proposed modifications to External Routable Connectivity allow for the use of Zero Trust Architecture or other network models that are not strictly perimeter or network-border based by removing the concepts of "inside" or "outside." These concepts are replaced with the language "through its Electronic Security Perimeter." The External Routable Connectivity term is used throughout the CIP Reliability Standards within the Applicable Systems column as a scoping mechanism based on the inherent risk associated with External Routable Connectivity as well as to limit the scope of requirements that would require External Routable Connectivity to function. The Project 2016-02 drafting team maintains this use of External Routable Connectivity, but also clarifies the relationship between External Routable Connectivity and Interactive Remote Access in that a non-routable, serial-only BES Cyber System (thus with no Electronic Security Perimeter) may have Interactive Remote Access through a subsequent internet protocol-to-serial conversion, as further discussed in this section.

Electronic Security Perimeter

The proposed revisions to the definition of Electronic Security Perimeter, shown in blackline, are as follows:

> The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol~~.~~**; or a logical boundary defined by one or more Electronic Access Points**.

In developing additional language to define an Electronic Security Perimeter, the Project 2016-02 drafting team accommodates other security models. The Project 2016-02 drafting team retained the "logical border surrounding a network" concept and added the "logical boundary" language to accommodate other models. The intent behind this is that a border surrounds an object (i.e., a network), but a boundary may not surround or enclose; it is a line that can be crossed, such as a policy enforcement point controlling access to a resource.

Interactive Remote Access (IRA)

The proposed revisions to the definition of Interactive Remote Access, shown in blackline, are as follows:

> User-initiated **electronic** access by a person ~~employing a remote access client or other remote access technology~~ using a **bi-directional** routable protocol**:**~~. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants.~~
>
> - **To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);**
> - **That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or**
> - **To a Management Interface.**
>
> Interactive ~~r~~**R**emote ~~a~~**A**ccess does not include**:**
>
> - **Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or**
> - ~~s~~**S**ystem-to-system process communication~~s~~.

The proposed revisions to Interactive Remote Access address both virtualization concepts and the needed clarifications identified during implementation (as described in Section IV.B in this petition). The proposed definition includes three instances where Interactive Remote Access exists and two exclusions. To address virtualization, the Project 2016-02 drafting team added accessing a Cyber System (thereby incorporating Virtual Cyber Assets and Shared Cyber Infrastructure) or a Management Interface (such as the Shared Cyber Infrastructure "console") as a type of Interactive Remote Access. In addition, the Project 2016-02 drafting team changed references to an Electronic Security Perimeter to reflect it is only one type of Interactive Remote Access instead of all types being defined as going through an Electronic Security Perimeter. Finally, the proposed modifications clarify that conversions of routable protocol to non-routable protocol by the Responsible Entity constitutes Interactive Remote Access to a Cyber System.

The exclusions carry forward constructs that already were not included in the currently enforceable definition of Interactive Remote Access.

Intermediate System

The proposed revisions to the definition of Intermediate System, shown in blackline, are as follows:

> **~~A Cyber Asset~~ One** or **~~collection of Cyber Assets performing access control~~ more Electronic Access Control or Monitoring Systems that are used** to restrict Interactive Remote Access to only authorized users. **~~The Intermediate System must not be located inside the Electronic Security Perimeter.~~**

The proposed modifications to the Intermediate System definition remove requirement language (i.e., where an Intermediate System must reside). The drafting team proposes moving that language to proposed CIP-005-8, Requirement R2, as further discussed in Section IV.E.5. The proposed modifications also update the definition from using "Cyber Asset" to using "EACMS" to reflect the other possible forms (i.e., Virtual Cyber Asset) of an Intermediate System. The proposed revisions also move the clarification of "[t]his includes Intermediate Systems" out of the EACMS definition into the Intermediate System definition.

Management Interface

Management Interface is a new proposed definition and reads as follows:

> **An administrative interface that:**
> - **Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure;**
> - **Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or**
> - **Configures an Electronic Access Point.**

In defining Management Interface, the Project 2016-02 drafting team provided a means for requirements to apply to the management plane that is responsible for managing Cyber Systems.

Protected Cyber Asset (PCA)

The proposed revisions to the definition of Protected Cyber Asset, shown in blackline, are as follows:

> One or more Cyber Assets **or Virtual Cyber Assets (VCA) that:** ~~**connected using a routable protocol within or on**~~
>
> - **Are protected by** an Electronic Security Perimeter **(ESP)** ~~**that is**~~ **but are** not part of the highest impact BES Cyber System **(BCS)** ~~**within**~~ **protected by** the same **ESP; or** ~~**Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.**~~
> - **Share CPU resources or memory resources with any part of the BCS, excluding VCA that are being actively remediated in an environment that isolates routable connectivity from BCS;**
>
> **Excluding Transient Cyber Assets.**

The proposed modifications to the Protected Cyber Asset definition ensure certain risks in a virtualized environment were mitigated through the protections applied to a Protected Cyber Asset. The Protected Cyber Asset definition exists to identify other Cyber Assets or Virtual Cyber Assets that must be protected by various CIP requirements due to what they share with a BES Cyber System. With virtualization, the Protected Cyber Asset definition was modified to include “share CPU resources or memory resources with any part of the BCS” to mitigate the risks of hardware-based vulnerabilities (e.g., Spectre, Meltdown, Rowhammer, Zenbleed, etc.) on Shared Cyber Infrastructure. Finally, the proposed modifications account for “remediation Virtual Local Area Network” automation of security controls where a Virtual Cyber Asset may instantiate in a logical network reserved for vulnerability assessment and updates but should not be considered a Protected Cyber Asset while temporarily in this state as its being updated prior to being connected to its production network.

Shared Cyber Infrastructure (SCI)

Shared Cyber Infrastructure is a new proposed definition and reads as follows:

> **One or more programmable electronic devices, including the software that shares the devices' resources, that:**
>
> - **Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or**
> - **Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.**
>
> **SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.**

The proposed term Shared Cyber Infrastructure was defined to separate the underlying hardware from Virtual Cyber Assets in the situation where the shared hardware resources support Virtual Cyber Assets of varying impact levels. This allows security requirements to be targeted to Shared Cyber Infrastructure to address the unique risks of shared hardware. There are many requirements that now include the newly defined term Shared Cyber Infrastructure ("SCI") in the "Applicable Systems" column to maintain security level parity with traditional Cyber Assets.

Virtual Cyber Asset

Virtual Cyber Asset is a new proposed definition and reads as follows:

> **A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure (SCI).**
>
> **Virtual Cyber Assets (VCAs) do not include:**
>
> - **Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems;**

- **<u>Dormant file-based images that contain operating systems or firmware; or</u>**
- **<u>SCI or Cyber Assets that host VCAs.</u>**

<u>Application containers are considered software of VCAs or Cyber Assets.</u>

The proposed definition of Virtual Cyber Asset provides clarity around those virtualized assets that do not have a one-to-one relationship between software and hardware. It also provides clarity on when certain behaviors of virtualized technologies are considered akin to a Cyber Asset within the CIP Reliability Standards.

2. Reliability Standard CIP-002-7

Consistent with the prior Version 5 framework, proposed Reliability Standard CIP-002-7 requires Responsible Entities to identify and categorize their BES Cyber Systems into low, medium, and high impact based on the assets (e.g., Control Centers, Transmission stations and substations, etc.) these BES Cyber Systems support. Attachment 1 to proposed CIP-002-7 includes criteria that categorize BES Cyber Systems based on the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. This categorization approach is still based on the NIST Risk Management framework, as developed to meet directives in Order No. 706.[50]

The proposed revisions in CIP-002-7 are minor, mostly aligning the standard with updates to the NERC Glossary. In addition to those mostly conforming changes, the proposed revisions incorporate the CIP-002-5.1a interpretation regarding "shared BES Cyber Systems" by clarifying that each "discrete" shared BES Cyber System meets medium impact rating 2.1 in Attachment 1 to CIP-002-7. This is consistent with Section 7.2.3 of the Standard Processes

---

[50] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *order on clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009), *order deny'g request for clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

Manual (Development of an Interpretation)[51] to incorporate an interpretation into the body of a Reliability Standard once that Reliability Standard is subsequently open for revision in a development project. A clean and redline version of proposed CIP-002-7 is included in **Exhibit A-1**, with additional technical rationale provided in **Exhibit E-1**.

3. Reliability Standard CIP-003-10

Proposed Reliability Standard CIP-003-10 requires Responsible Entities to develop cyber security policies to help establish responsibility and accountability through all levels of an organization. In addition, this standard includes the cyber security requirements applicable to assets containing low impact BES Cyber Systems. The proposed revisions align the requirements with updates to the NERC Glossary and apply low impact requirements to virtualized technologies through new proposed terms such as "Shared Cyber Infrastructure" and "Virtual Cyber Asset." A clean and redline version of proposed CIP-003-10 is included in **Exhibit A-2**, with additional technical rationale provided in **Exhibit E-2**.

4. Reliability Standard CIP-004-8

Proposed Reliability Standard CIP-004-8 minimizes the risk of individuals inappropriately accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management. Proposed Reliability Standard CIP-004-8 includes six requirements: (1) Requirement R1 requires a Responsible Entity to implement a documented security awareness process for high and medium impact BES Cyber Systems that reinforces cyber security practices for certain personnel; (2) Requirement R2 requires Responsible Entities to implement a cyber security training program that includes the applicable requirement parts; (3) Requirement R3 requires a documented personnel risk

---

[51] The NERC Standard Processes Manual is available at https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix_3A_SPM_Clean_Mar2019.pdf.

assessment program(s); (4) Requirement R4 requires a documented access management program(s) that includes the applicable requirement parts; (5) Requirement R5 requires a documented access revocation program(s) that includes the applicable requirement parts; and (6) Requirement R6 requires an access management program(s) to authorize, verify, and revoke provisioned access to BES Cyber System Information that includes the applicable requirement parts.

The proposed revisions in CIP-004-8 add Shared Cyber Infrastructure as an applicable system to help ensure infrastructure that supports virtualized technologies receives appropriate CIP personnel and training protections. In addition, the proposed revisions clarify applicability to medium impact BES Cyber Systems with External Routable Connectivity and those with Interactive Remote Access. A clean and redline version of proposed CIP-004-8 is included in **Exhibit A-3**, with additional technical rationale provided in **Exhibit E-3**.

5. Reliability Standard CIP-005-8

Proposed Reliability Standard CIP-005-8 includes requirements around controlling electronic access to medium and high impact BES Cyber Systems. The standard requires Responsible Entities to develop an Electronic Security Perimeter that only permits certain communications to medium and high impact BES Cyber Systems. Through revisions to the Electronic Security Perimeter definition and requirements to focus on the security objective of permitting only necessary communication through the Electronic Security Perimeter, the proposed standard allows Responsible Entities to implement security models at a more granular level in addition to network perimeter-based solutions (e.g., firewalls) to control these communications. While the proposed Reliability Standard no longer limits Responsible Entities to using a perimeter-based model, Responsible Entities may continue to meet the security objective of the requirement by deploying such a configuration. However, Responsible Entities may also deploy controls on communications that can be on a per-access or per-session level.

a. Requirement R1

Proposed Requirement R1 of CIP-005-8 requires Responsible Entities to implement one or more documented processes regarding Electronic Security Perimeters. As described below, the proposed revised requirement parts incorporate a security objective approach to accommodate more security models.

The drafting team revised the language "shall reside within" an ESP to "must be protected by an ESP." Through this change, the proposed Requirement R1, Part 1.1 better accommodates architectures without a "perimeter," where the concepts of inside and outside such perimeter do not work. The language, however, still accommodates "traditional" Open Systems Interconnection[52] Layer 3 firewalls in that communications would go "through" the access point in the firewall that establishes the Electronic Security Perimeter.

Proposed Requirement R1, Part 1.2 removes an explicit requirement to use an Electronic Access Point to control communications to applicable systems but replaces it with core security objectives of permitting "only needed routable communications" through the Electronic Security Perimeter and denying all others (excluding time sensitive communications of Protection Systems). This security objective focuses on the "reachability" of applicable systems, permitting Responsible Entities to use Electronic Access Points to control the accessibility of the applicable systems, among other controls. This requirement part incorporates aspects of the previous CIP-005-7, Requirement R1, Part 1.3 into the security objective. In addition, this requirement part

---

[52] The Open Systems Interconnection ("OSI") model is often cited in information security and was developed by the International Organization for Standardization. The OSI model is seven conceptual "layers" that define how communications between systems can occur: 1) physical, 2) data link, 3) network, 4) transport, 5) session, 6) presentation, and 7) application. Wikipedia, *OSI Model*, https://en.wikipedia.org/wiki/OSI_model.

now explicitly requires a Responsible Entity to document the reason for granting access to help ensure only needed communications are permitted.

Proposed Requirement R1, Part 1.3 includes a security objective to protect the configurations of Electronic Security Perimeters and Shared Cyber Infrastructure. To achieve this objective, the requirement part applies to Electronic Access Control or Monitoring Systems that control and create the Electronic Security Perimeter for Applicable Systems in Requirement R1, Part 1.1 and Shared Cyber Infrastructure supporting an Applicable System in Requirement R1, Part 1.1. The intent behind separating this requirement part from the protections in Requirement R1, Part 1.2 is to clarify that entities do not need an Electronic Access Control or Monitoring System for each Electronic Access Control or Monitoring System.

Proposed Requirement R1, Part 1.4 adds "SCI supporting an Applicable System in this Part" to the scope of the requirement part to ensure that controls regarding Dial-up Connectivity are also applicable to Virtual Cyber Assets and Shared Cyber Infrastructure; and "where technically feasible" has been replaced with the "per system capability" language.

The revisions in proposed Requirement R1, Part 1.5 remove the prescriptive application of protections to the Electronic Access Points and now require malicious routable protocol communications detection entering or leaving the Electronic Security Perimeter.

Proposed Requirement R1, Part 1.6 addresses the issue colloquially known as "Super ESPs," where high or medium impact BES Cyber Systems at Control Centers extend a single Electronic Security Perimeter beyond one Physical Security Perimeter. This often applies to virtualized Control Center environments that implement network adjacency to allow workloads to automatically move from one physical location to another to increase BES Cyber System resiliency between primary and backup Control Centers. The security objective is to protect the confidentiality and integrity of the data traversing communication links used to span a single Electronic Security Perimeter between multiple Physical Security Perimeters. This requirement part works in conjunction with the new Applicability Section 4.2.3.3 exemption in the CIP Reliability Standards: proposed Part 1.6 protects the confidentiality and integrity of the data (typically through encryption) between Physical Security Perimeters, while the exemption section covers related Cyber Systems between those encryption points but does not exclude the endpoints performing the encryption. Therefore, those endpoints performing encryption would be covered by the CIP Reliability Standards requirements.

Also, the former CIP-006-6, Requirement R1, Part 1.10 has been removed and incorporated into this new Requirement R1, Part 1.6 requirement part; consolidating the protections of an Electronic Security Perimeter and its components that extend outside of a Physical Security Perimeter within one standard. Communications equipment associated with communications links (e.g., equipment belonging to carriers) is exempted from the CIP Reliability Standards with the Applicability Section 4.2.3.2 exemption. However, that only applies to equipment between discrete Electronic Security Perimeters. In this extended Electronic Security Perimeter situation where a single Electronic Security Perimeter spans multiple sites or Physical Security Perimeters, that exemption does not apply and the potential exists for data to traverse a connection that uses third-party communications equipment that is unprotected *inside* an Electronic Security Perimeter. As a result, there is a need to enforce confidentiality and integrity controls (such as encryption) on the data that traverses Physical Security Perimeters while within the same Electronic Security Perimeter to isolate any protected data from access through the communications equipment. This consolidation also incorporates cabling and non-programmable communication components that are not protected by a Physical Security

Perimeter, intending to protect data moving across the state as well as data traversing cabling that crosses the hall outside of the Physical Security Perimeter.

b. Requirement R2

Proposed Requirement R2 governs protections around remote access management, specifically Interactive Remote Access, used to support and maintain control systems networks. The proposed revisions to Requirement R2 adapt these protections to support virtualized configurations and clarify issues around defining Interactive Remote Access that arose during implementation of the Version 5 CIP Reliability Standards. Similar to proposed Requirement R1, the following revised requirement parts in proposed Requirement R2 incorporate a security objective approach to accommodate more security models:

Proposed Requirement R2, Part 2.1 expands safeguards for remote access to Shared Cyber Infrastructure in addition to high and medium impact BES Cyber Systems. The Project 2016-02 drafting team simplified the requirement part language in conjunction with the clarified terms of Interactive Remote Access and Intermediate System.

The revisions in proposed Requirement R2, Part 2.2 change the applicability to clarify protections should be applied between the Intermediate System and the remote client rather than between the Intermediate System and the BES Cyber System. In addition, proposed Requirement R2, Part 2.2 changed from a technically specific requirement for encryption to an objective-based requirement to protect the confidentiality and integrity of the Interactive Remote Access session.

Proposed Requirement R2, Part 2.3 clarifies that multi-factor authentication should be applied to the Intermediate System through changes to applicable systems.

Proposed Requirement R2, Parts 2.4 and 2.5 are supply chain protections for vendor remote access sessions. There were only acronym changes and the addition of Shared Cyber Infrastructure to applicability for these requirement parts.

Proposed Requirement R2, Parts 2.6 and 2.7 are new requirement parts focusing on reducing the attack surface between an Intermediate System and the BES Cyber System. Proposed Requirement R2, Part 2.6 is intended to prevent a virtualized Intermediate System from sharing central processing units or memory with the BES Cyber System for which it controls access to reduce the risk for a side-channel attack to other Virtual Cyber Assets sharing those resources. Proposed Requirement R2, Part 2.7 requires that routable protocol communications between Intermediate Systems and applicable systems in Part 2.1 must be through an Electronic Security Perimeter. This requirement part replaces the language in the currently enforceable definition of Intermediate System that stated an Intermediate System "must not be located inside" the Electronic Security Perimeter.

c. Requirement R3

Finally, proposed Requirement R3 applicability was updated to extend the protections for vendor-initiated remote connections to Shared Cyber Infrastructure. A clean and redline version of proposed CIP-005-8 is included in **Exhibit A-4**, with additional technical rationale provided in **Exhibit E-4**.

6. Reliability Standard CIP-006-7

Proposed Reliability Standard CIP-006-7 requires a physical security plan to manage physical access to BES Cyber Systems. These requirements are different than the physical security requirements in CIP-014 in that CIP-006 is centered on access to the BES Cyber Systems whereas CIP-014 focuses on physical security of critical infrastructure itself (e.g., security around substations). The proposed revisions apply certain physical protection requirements to virtualization infrastructure where appropriate. A clean and redline version of proposed CIP-006-7 is included in **Exhibit A-5**, with additional technical rationale provided in **Exhibit E-5**.

7. Reliability Standard CIP-007-7

Proposed Reliability Standard CIP-007-7 specifies technical, operational, and procedural requirements to manage system security (e.g., malicious code prevention methods, patch management, etc.). The proposed revisions focus on security objectives rather than specific controls for system security management to accommodate virtualized environments. The revised standard also includes Shared Cyber Infrastructure as an applicable system in all requirement parts of CIP-007-7. The proposed revisions also include a new requirement applicable to Shared Cyber Infrastructure that mitigates vulnerabilities in using the same hardware for different impact categorizations. Finally, the proposed revisions also use "per system capability" instead of "where technically feasible."

Proposed Requirement R1 has an updated table name, "System Hardening" (changed from "Ports and Services"), to reflect the security objective of reducing applicable systems' attack surface. Similarly, proposed Requirement R1, Part 1.1 changes its focus from enabling or restricting ports to the broader focus of disabling or preventing unneeded routable protocol network accessibility. In some instances, a Responsible Entity may be able to disable a service or remove or uninstall software that is providing unneeded network accessibility to the applicable system. In other instances, a Responsible Entity may not be able to disable a service but can prevent access to it in another layer, such as the underlying operating system with a host-based firewall, a policy enforcement point, or other means of filtering traffic. The phrase "per system capability" means that if a Responsible Entity can demonstrate that the applicable system is incapable of performing a required action (e.g., a firmware-based "black box" device with limited configuration capabilities), the requirement is conditional on the ability of the applicable system.

As noted above, proposed Requirement R1, Part 1.3 is a new requirement part applicable to Shared Cyber Infrastructure that supports high or medium impact BES Cyber Systems or their associated Protected Cyber Assets. The intent of proposed Requirement R1, Part 1.3 is to mitigate the risk of exploitation of vulnerabilities of any shared central processing unit resources or memory resources supporting medium or high impact BES Cyber Systems and their associated Protected Cyber Assets. Proposed Requirement R1, Part 1.3 achieves this objective by requiring Responsible Entities to prevent the sharing of these resources, excluding storage resources, with Virtual Cyber Assets that are not, or are not associated with, a medium or high impact BES Cyber System.

The remaining requirements in proposed Reliability Standard CIP-007-7 (Requirements R2, R3, R4, and R5) include minor, conforming changes and the changes listed above (adding Shared Cyber Infrastructure in the Applicable Systems column and replacing "where technically feasible" with "per system capability"). A clean and redline version of proposed CIP-007-7 is included in **Exhibit A-6**, with additional technical rationale provided in **Exhibit E-6**.

8. Reliability Standard CIP-008-7

Proposed Reliability Standard CIP-008-7 specifies incident response requirements to mitigate the risk to the reliable operation of the Bulk Electric System resulting from a Cyber Security Incident. The proposed revisions add Shared Cyber Infrastructure to the applicable systems for incident response requirements. A clean and redline version of proposed CIP-008-7 is included in **Exhibit A-7**, with additional technical rationale provided in **Exhibit E-7**.

9. Reliability Standard CIP-009-7

Proposed Reliability Standard CIP-009-7 specifies recovery plan requirements to recover reliability functions of BES Cyber Systems. The proposed revisions add Shared Cyber Infrastructure to the applicable systems where appropriate. A clean and redline version of proposed CIP-009-7 is included in **Exhibit A-8**, with additional technical rationale provided in **Exhibit E-8**.

10. Reliability Standard CIP-010-5

Proposed Reliability Standard CIP-010-5 governs change management requirements and vulnerability assessment requirements for medium and high impact BES Cyber Systems. The proposed revisions broaden the change management requirements by incorporating the security objective of controlling the implementation of intended changes to software or settings that could weaken certain cyber security controls rather than only permitting a baseline configuration. While Responsible Entities may continue using a baseline configuration to manage change, Responsible Entities may now focus management around those changes that impact the security behavior of certain controls. This accounts for the dynamic nature of virtual machines and other virtualized technologies by permitting authorization of a change for automatic updates that will occur in the future when these virtual machines or application containers instantiate. This contrasts with only looking "backwards" at changes to a baseline as is used for non-virtual machines that run 24 hours a day, seven days a week. In addition, the proposed revisions add Shared Cyber Infrastructure to applicability where appropriate and replace "where technically feasible" with "per system capability."

a. Requirement R1

Like currently enforceable CIP-010-4, the objective of proposed Requirement R1 remains to prevent unauthorized changes to BES Cyber Systems. Recognizing the true security objective behind change management, proposed Requirement R1 focuses on authorizing intended changes that alter security behaviors rather than focusing on listing and documenting changes. In a dynamic environment such as virtualization, where a Virtual Cyber Asset may lie dormant but automatically patched at a future instantiation, the goal of change management is to ensure any changes are authorized prior to that instantiation, not tracking the time and date when the patching occurs for each instantiation with an update to the baseline 30 days later. As a result, the focus of proposed Requirement R1 has changed from documenting the installed software and its open ports on a Cyber Asset or Virtual Cyber Asset at some point post-change to authorizing the changes that will occur when it does instantiate, which provides more security value for virtualized environments. As noted previously, Responsible Entities may continue to use baseline configurations as a valid way to meet Requirement R1.

The Project 2016-02 drafting team replaced the baseline language in proposed Requirement R1, Part 1.1 to focus on the authorization of changes (previously in Requirement R1, Part 1.2). When reviewing the five components that comprised a baseline configuration in the current Part 1.1 (operating system or firmware, commercially available or open source application software intentionally installed, custom software installed, ports, and patches), the Project 2016-02 drafting team determined that the protections around each of these items were already required in the technical controls of CIP-005 and CIP-007. As such, change management requirements in Requirement R1, Part 1.1 needed to not just focus on documenting changes to those controls but rather control the authorization of those changes. To that end, proposed Requirement R1, Part 1.1 requires Responsible Entities to authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural or physical controls, serving one or more requirement parts in

CIP-005 and CIP-007, as defined by the Responsible Entity. With this revision, aspects of current Requirement R1, Parts 1.2 and 1.3, which both relate to using a baseline configuration for change management, are incorporated into the security objective of proposed Requirement R1, Part 1.1.

With the consolidation of current Requirement R1, Parts 1.1 through 1.3 into the security objective of proposed Requirement R1, Part 1.1, proposed Requirement R1, Part 1.2 is a revised current Requirement R1, Part 1.5. The revisions are mostly conforming in that they remove references to baseline configuration and remove the "where technically feasible" language. Instead of "where technically feasible" language, the drafting team determined a CIP Exceptional Circumstance more appropriate to support Responsible Entities' recovering from events or conditions more swiftly.

Proposed Requirement R1, Part 1.3 now maps to the current Requirement R1, Part 1.6, one of the supply chain requirements to verify the integrity of software and the identify of its source. The proposed revisions to Requirement R1, Part 1.3 are mostly conforming, with removal of references to baseline configuration.

Based on the identification of controls in CIP-005 and CIP-007 in proposed Requirement R1, Part 1.1, proposed Requirement R1, Part 1.4 simplifies the current requirement to ensure that altered controls in those standards are not adversely affected. The drafting team also added the language "as part of the changes authorized per Requirement R1, Part 1.1" to indicate that a Responsible Entity should verify that the controls are not adversely affected before closing out those changes.

b. Requirement R2

The modifications in proposed Requirement R2 adjust the scope of configuration monitoring requirements to conform with revisions to Requirement R1 and support the additional Applicable System (SCI supporting high impact BES Cyber Systems and associated EACMS and PCA). To achieve this scope adjustment, proposed Requirement R2, Part 2.1 requires Responsible Entities to implement methods to monitor certain unauthorized changes that affect Applicable Systems. The unauthorized changes subject to monitoring under Requirement R2, Part 2.1 are those changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity. Such entity-defined controls must include at least one cyber security control for each of the following seven controls: (1) Configuration on each Applicable System that affects its routable protocol network accessibility; (2) Configuration of CPU or memory sharing of Virtual Cyber Assets on Shared Cyber Infrastructure; (3) Installation, removal, and update of operating system, firmware, software, and cyber security patches; (4) Configuration of malicious code protection methods; (5) Configuration of security event logging or alerting; (6) Configuration of authentication methods; and (7) Changes to the enabled or disabled status of accounts. The Project 2016-02 drafting team added "per system capability" to indicate that an Applicable System may not have one of the seven controls configured on an applicable system (e.g., there may be no sharing of Virtual Cyber Assets on a Shared Cyber Infrastructure), so a Responsible Entity would not be expected to monitor controls it does not have. Proposed Requirement R2, Part 2.1 retains the requirement to document and investigate detected unauthorized changes.

In scoping the controls subject to monitoring, the drafting team focused on a subset of the controls at the center of proposed Requirement R1, Part 1.1. The intent behind this was to focus change management on those controls responsible for maintaining a Cyber System's security posture, such as those supporting systems security management in proposed CIP-007-7. The Project 2016-02 drafting team also determined these controls likely had the capability for automated monitoring.

The Project 2016-02 drafting team used the phrase "that include at least one cyber security control for each of the following" to allow Responsible Entities to monitor a primary security control if they have multiple overlapping controls. The Project 2016-02 drafting team's intent is that having multiple security controls over these categories is a good and beneficial practice where possible, and entities should not be discouraged from having more than one. This allows the Responsible Entity to choose the primary control it monitors for unauthorized changes. The Responsible Entity may of course monitor more than one, but one is required.

Additionally, the Project 2016-02 drafting team added "per system capability" in recognition that not all changes in scope can be monitored on every Cyber System. The intent is not for the 'per system capability' language to exclude manual monitoring methods from the scope of proposed Part 2.1. Rather, the Project 2016-02 drafting team's intent when using the "per system capability" language is to keep the scope of Requirement R2 to those things for which automated solutions are available and more likely to be monitored and alerted for changes. To that end, the word "system" in "per system capability" refers to the Applicable Systems for the requirement, and not the capability of the automated tool used to monitor. As a result, the "per system capability" language does not absolve Responsible Entities of the obligation to implement monitoring methods where automated solutions have not been implemented.

Accordingly, manual methods to accomplish the same results where automated monitoring cannot be done remains a requirement where the Applicable System is capable of producing data related to the list of seven cyber security-related categories to monitor.

c. Requirement R3

Proposed Requirement R3 requires Responsible Entities to implement a process regarding vulnerability assessments of Applicable Systems. Proposed Requirement R3, Parts 3.1 and 3.2 add Shared Cyber Infrastructure as an Applicable System and include conforming changes to reflect the change from only requiring baseline configurations. Proposed Requirement R3, Part 3.3 includes revisions that reflect the dynamic nature of virtualized technologies. As such, the proposed requirement part requires the vulnerability assessment at a point prior to the Virtual Cyber Asset being instantiated, with the "production" connectivity it requires, to perform its function either as a part of a BES Cyber System, as an Electronic Access Control or Monitoring System, or as a Protected Cyber Asset. As it begins to perform those functions of Applicable Systems, it becomes an "Applicable System" at that point, and the Responsible Entity should have already performed the vulnerability assessment. In the case of a remediation Virtual Local Area Network, this may be performed automatically at every instantiation. The proposed change recognizes that Virtual Cyber Assets do not need to be created first in a separate hardware environment and then somehow imported when the vulnerability assessment can safely be performed in a "production environment."

d. Requirement R4

Proposed Requirement R4 requires Responsible Entities to implement a plan to manage Transient Cyber Assets and Removable Media. The proposed revisions within Requirement R4 are mostly conforming and add the term Shared Cyber Infrastructure where appropriate. The proposed revisions within Attachment 1 to Requirement R4 also align language with that in Attachment 1 of proposed CIP-003-10. A clean and redline version of proposed CIP-010-5 is included in **Exhibit A-9**, with additional technical rationale provided in **Exhibit E-9**.

11. Reliability Standard CIP-011-4

Proposed Reliability Standard CIP-011-4 specifies information protection requirements to safeguard BES Cyber System Information. The proposed revisions add information protection requirements to Shared Cyber Infrastructure and apply reuse and disposal requirements at a system versus asset level. Proposed Requirement R1 requires Responsible Entities to implement a documented information protection program(s) that includes the applicable requirement parts. Proposed Requirement R2 requires Responsible Entities to implement documented processes regarding BES Cyber Asset reuse and disposal, consistent with the applicable requirement parts. A clean and redline version of proposed CIP-011-4 is included in **Exhibit A-10**, with additional technical rationale provided in **Exhibit E-10**.

12. Reliability Standard CIP-013-3

Proposed Reliability Standard CIP-013-3 requires Responsible Entities to consider and address cyber security risks from vendor products or services during planning for the procurement of BES Cyber Systems as well as Electronic Access Control or Monitoring Systems and Physical Access Control Systems. Proposed Reliability Standard CIP-013-3 includes three requirements: (1) Requirement R1 requires a Responsible Entity to develop documented supply chain cyber security risk management plan(s) and includes requirement parts detailing the processes to include in the plan; (2) Requirement R2 requires Responsible Entities to implement the plan(s); and (3) Requirement R3 requires review and CIP Senior Manager, or delegate, approval of the plan(s) at least once every 15 calendar months. The proposed revisions extend these supply chain risk management requirements to Shared Cyber Infrastructure. A clean and redline version of proposed CIP-013-3 is included in **Exhibit A-11**, with additional technical rationale provided in **Exhibit E-11**.

F. Other Modifications

To facilitate the proposed changes discussed in Sections IV.A through IV.E supra, there were several other modifications throughout the CIP Reliability Standards that are clarifying or conforming changes but not as substantive as other revisions described in Section IV. For example, the drafting team proposes clarifications of the term "between discrete Electronic Security Perimeters" by modifying the Applicability exemptions section of the CIP Reliability Standards to add Section 4.2.3.3. The proposed section recognizes that the ability to move workloads or virtual machines across different sites for increased resiliency can require different sites to be connected as a flat network without layer 3 Electronic Security Perimeters at each discrete site (e.g., a layer 2 adjacency across the sites). As a result, a "super ESP" is created across the sites and thus an exemption based on having a discrete layer 3 Electronic Security Perimeter at each site no longer works to exclude, for example, the network transport equipment that may belong to carriers, which was the intent behind current Applicability Section 4.2.3.2.

As described above in Section IV.E.5, when extending an Electronic Security Perimeter between geographic locations, the requirement in proposed CIP-005-8 to protect the confidentiality and integrity of the data (typically through encryption) between the relevant Physical Security Perimeters applies. This exemption in proposed Applicability Section 4.2.3.3 then covers the related Cyber Systems "between" those encryption points but does not exclude the endpoints performing the encryption.

There are several other revisions throughout the proposed standards that are administrative in nature, such as use of acronyms, streamlining the Violation Severity Levels, removing functional entities no longer subject to Reliability Standards, and removing the non-enforceable Background and Guidelines and Technical Basis sections to separate technical rationale documents.

In addition, as proposed Reliability Standards CIP-002-7, CIP-006-7, CIP-007-7 and CIP-009-7 have not been modified in several years, there are some more administrative updates within those standards. As such, the proposed Reliability Standards contain a number of minor modifications to align the standard with revisions to other standards or initiatives in other areas. These changes are shown in clean and redline in **Exhibits A-1, A-5, A-6, and A-8** and are summarized below.

First, the proposed modifications would remove Interchange Coordinator or Interchange Authority from the Applicability section of proposed Reliability Standards CIP-002-7, CIP-006-7, CIP-007-7, and CIP-009-7. This revision is consistent with FERC-approved changes to the NERC Compliance Registry under the risk-based registration initiative.[53]

Second, the proposed modifications replace the term "Special Protection Systems" with the term "Remedial Action Schemes," consistent with similar revisions made to other NERC Reliability Standards.[54] This change occurs in the following locations:

- Applicability subsections 4.1.2.2 and 4.2.1.2 in proposed CIP-002-7, CIP-006-7, CIP-007-7, and CIP-009-7;
- Proposed CIP-002-7, Requirement R1;

---

[53] *N. Am. Elec. Reliability Corp.*, 150 FERC ¶ 61,213 (2015) (approving removal of the Purchasing Selling Entity and Interchange Authority/Coordinator from the NERC Compliance Registry).

[54] In Order No. 818, the Commission approved NERC's revised definition of the term "Remedial Action Scheme" and approved certain Reliability Standards in which references to the term "Special Protections Systems" were removed and replaced with the term "Remedial Action Schemes." *Revisions to Emergency Operations Reliability Standards; Revisions to Undervoltage Load Shedding Reliability Standards; Revisions to the Definition of "Remedial Action Scheme" and Related Reliability Standards*, Order No. 818, 153 FERC ¶ 61,228 (2015).

- Proposed CIP-002-7, Attachment 1, medium impact rating criterion 2.9; and
- Proposed CIP-002-7, low impact rating criterion 3.5.

Finally, proposed CIP-002-7, Requirement R2 begins with the word "**Each** Responsible Entity shall:", instead of "~~**The**~~ Responsible Entity shall:", to conform with Requirement R1 language and other requirements in the CIP suite of standards.

G. Enforceability of Proposed Reliability Standards

The proposed Reliability Standards also include measures that support each requirement by clearly identifying what is required and how NERC and the Regional Entities will enforce the requirement. These measures help ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.[55] Additionally, the proposed Reliability Standards include VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC and the Regional Entities will enforce the requirements of the proposed Reliability Standards. The VRFs and VSLs for the proposed Reliability Standards comport with NERC and Commission guidelines related to their assignment. **Exhibit F** provides a detailed review of the VRFs and VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines.

As the proposed Reliability Standards incorporate security objectives into requirements, the Compliance Monitoring and Enforcement Program[56] processes and procedures provide effective tools for monitoring and enforcing those security objectives. NERC and the Regional Entities will use existing risk-based compliance monitoring processes to effectively monitor compliance with the new Reliability Standards requirements. As with any new Reliability

---

[55] Order No. 672 at P 327.

[56] NERC, *Rules of Procedure*, Section 400 et. seq.; Appendices 4B and 4C, https://www.nerc.com/AboutNERC/RulesOfProcedure/NERC%20ROP%20effective%2020220825_with%20appendicies.pdf.

Standard, NERC and the Regional Entities expect to provide some training and collaboration on the security objectives to ensure that monitoring staff possess the necessary subject matter expertise to employ professional judgment in assessing compliance, consistent with applicable auditing principles.[57] In addition, NERC and the Regional Entities will consider using stakeholder engagement efforts, such as Small Group Advisory Sessions or entity assist visits, as appropriate, to help ensure both Responsible Entities and monitoring staff are prepared for implementation.

Should a Potential Noncompliance[58] go through enforcement processes for disposition, the existing enforcement processes provide effective means for assessing such findings in a fair and non-preferential manner. For each finding assessed, NERC and the Regional Entities consider the facts and circumstances surrounding each violation and use professional judgment to assess whether security objectives were met, consistent with the FERC-approved Sanction Guidelines.[59] This ensures that enforcement actions bear a reasonable relationship to the seriousness of the violation.[60] In applying such guidelines to requirements with security objectives, NERC and the Regional Entities can follow a repeatable process while ensuring each Responsible Entity is treated fairly based on the unique facts and circumstances of each Potential Noncompliance.

---

[57] United States Government Accountability Office, *Government Auditing Standards*, Requirement 3.109 (2024), https://www.gao.gov/assets/d24106786.pdf.

[58] *See N. Am. Elec. Reliability Corp. Definitions Used in the Rules of Procedure, Appendix 2 to the Rules of Procedure* (effective May 19, 2022) at 17 ("Potential Noncompliance" means the identification, by the Compliance Enforcement Authority, of a possible failure by a Registered Entity to comply with a Reliability Standard that is applicable to the Registered Entity), https://www.nerc.com/AboutNERC/RulesOfProcedure/ROP_Appendix%202_20220519.pdf.)

[59] *See Sanction Guidelines of the North American Electric Reliability Corporation* (effective January 19, 2021) at 3, https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix_4B_effective%2020210119.pdf .

[60] *Id.*

V. EFFECTIVE DATE

NERC respectfully requests that the Commission approve the proposed Reliability Standards and associated definitions to become effective as set forth in the proposed Implementation Plan, provided in **Exhibit B** hereto. The proposed Implementation Plan provides that the proposed Reliability Standards and definitions shall become effective on the later of: (1) April 1, 2026; or (2) the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Reliability Standards and definitions, or as otherwise provided for by the applicable governmental authority. The proposed implementation timeframe balances the urgency to implement the requirements with the time needed to develop any relevant capabilities.

The proposed Implementation Plan also permits Responsible Entities to elect to comply with the proposed Reliability Standards and associated definitions following Commission approval but prior to their effective date, provided the Responsible Entity notifies its applicable Regional Entities as stated in the Implementation Plan. This option allows Responsible Entities to implement the appropriate controls for virtualized technologies as soon as feasible or continue with configurations currently allowed under the CIP Reliability Standards but update their compliance documentation in a manner appropriate for their schedules. The early adoption dates are limited to three instances to better support Regional Entity tracking of Responsible Entities' availing themselves of this provision in the Implementation Plan:

> <u>Early adoption option 1</u>: First day of the first calendar quarter that is six (6) months after the effective date of the applicable governmental authority's order approving the proposed Reliability Standards and definitions
>
> <u>Early adoption option 2</u>: First day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the proposed Reliability Standards and definitions.

> Early adoption option 3: First day of the first calendar quarter that is eighteen (18) months after the effective date of the applicable governmental authority's order approving the proposed Reliability Standards and definitions.

In addition, the proposed Implementation Plan carries forward the planned and unplanned changes section that has been used in implementation plans associated with previous versions of the CIP Reliability Standards.

VI. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission approve:

- proposed Reliability Standards, and associated elements included in **Exhibit A**, effective as proposed herein;
- the proposed Implementation Plan included in **Exhibit B**; and
- the retirement of Reliability Standards effective as proposed herein.

Respectfully submitted,

/s/ Marisa Hecht
Lauren Perotti
Assistant General Counsel
Marisa Hecht
Senior Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
Marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: July 10, 2024

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A

Proposed Reliability Standards

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-1

Proposed Reliability Standard CIP-002-7
Clean

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the Bulk Electric System (BES). Identification and categorization of BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1. **Balancing Authority**

      4.1.2. **Distribution Provider that owns** one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

            4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-7:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of Parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;

ii. Transmission stations and substations;

iii. Generation resources;

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;

v. RAS that support the reliable operation of the BES; and

vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer of identified BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent but less than or equal to 10 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category;	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BCS, more than 10 percent but less than or equal to 15 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category;	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	fewer identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or fewer high or medium BCS have not been identified.	OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent but less than or equal to 10 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than five but less than or equal to 10 high or medium BCS have not been identified.	OR For Responsible Entities with a total of 100 or fewer high or medium impact BCS, more than 10 but less than or equal to 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 10 percent but less than or equal to 15 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than 10 but less than or equal to 15 high or medium BCS have not been identified.	than 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of high or medium impact BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BCS have not been identified.
R2	The Responsible Entity did not complete its review and update	The Responsible Entity did not complete its review and update	The Responsible Entity did not complete its review and update	The Responsible Entity did not complete its review and update

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (Part 2.2)	for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (Part2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (Part 2.2)	for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (Part 2.2)	for the identification required for Requirement R1 within 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (Part 2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-002-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced "Devices" with "Systems" in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
7	TBD	Virtualization Modifications	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High impact rating**

   Each BCS used by and located at any of the following:

   1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

   1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

   1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

   1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium impact rating**

   Each BCS, not included in Section 1 above, associated with any of the following:

   2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

   2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

   2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

   2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

   2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each RAS or automated switching System that operates BES Elements, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in high impact rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in high impact rating, above.

2.13. Each Control Center or backup Control Center, not already included in high impact rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low impact rating

BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Exhibit A-1

Proposed Reliability Standard CIP-002-7
Redline

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-~~5.1a~~7

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those ~~BES Cyber Systems~~BCS could have on the reliable operation of the ~~BES.~~Bulk Electric System (BES). Identification and categorization of ~~BES Cyber Systems~~BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

    4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. **Balancing Authority**

    4.1.2. **Distribution Provider that owns** one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and

including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

~~4.1.6.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. ~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme~~Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-~~5.1a~~7:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**5.**~~ **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan"

~~1. **24 Months Minimum –** CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

~~**6. Background:**~~

~~This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.~~

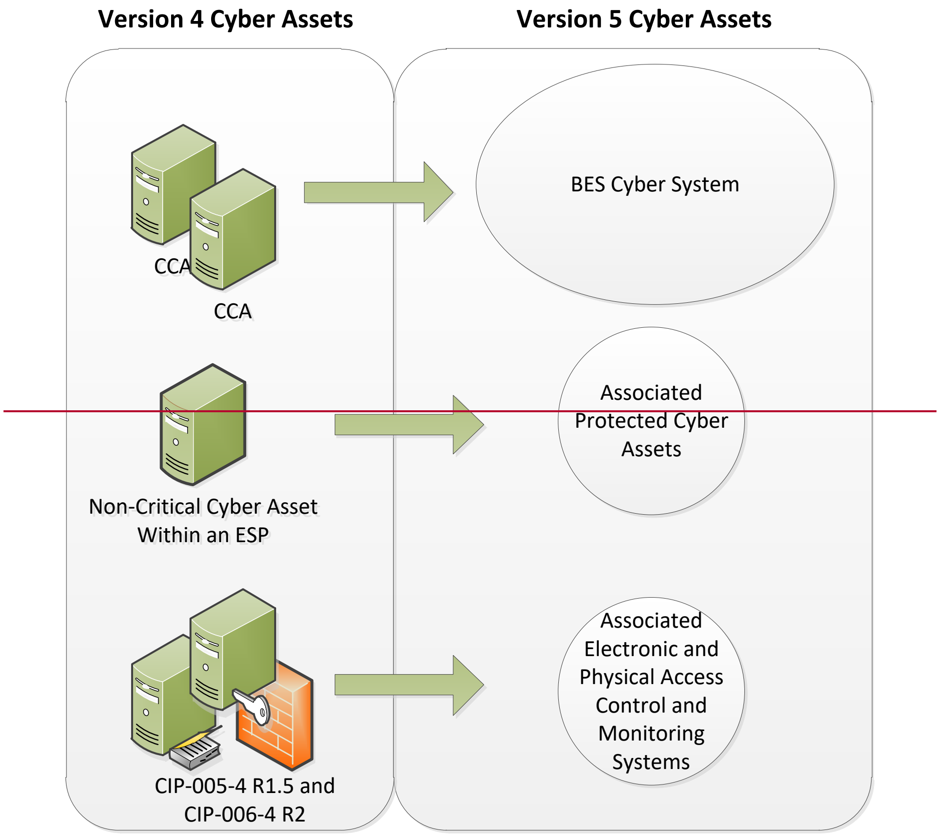
~~Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

5. ~~Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS,~~

~~which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~BES Cyber Systems~~

~~One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.~~



~~In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.~~

~~Another reason for using the term “BES Cyber System” is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.~~

~~It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Reliable Operation of the BES~~

~~The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity’s responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.~~

~~Real-time Operations~~

~~One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than “Real-time,” BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.~~

~~Categorization Criteria~~

~~The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES~~

~~Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.~~

~~This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.~~

~~Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems~~

~~BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:~~

> **~~Electronic Access Control or Monitoring Systems (“EACMS”)~~** ~~– Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.~~
>
> **~~Physical Access Control Systems (“PACS”)~~**~~– Examples include: authentication servers, card systems, and badge control systems.~~
>
> **~~Protected Cyber Assets (“PCA”)~~** ~~– Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of ~~parts~~Parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** ~~Special Protection Systems~~RAS that support the reliable operation of the ~~Bulk Electric System~~BES; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact ~~BES Cyber Systems~~BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact ~~BES Cyber Systems~~BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact ~~BES Cyber System~~BCS according to Attachment 1, Section 3, if any (a discrete list of low impact ~~BES Cyber Systems~~BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1~~, and Parts 1.1 and 1.2~~.

R2. ~~The~~Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1~~—~~ Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the~~ "Compliance Enforcement Authority ~~("CEA") unless the applicable~~" means NERC or the Regional Entity, or any entity ~~is owned, operated, or controlled~~as otherwise designated by ~~the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC~~ an Applicable Governmental Authority, in their respective roles of monitoring and/or ~~other applicable governmental authority shall serve as the CEA.~~enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Assessment Processes~~Enforcement Program:

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~
- ~~Complaint~~

~~**1.4. Additional Compliance Information**~~

- ~~None~~

~~2. Table of Compliance Elements~~

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-002-~~5.1a~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, five percent or fewer of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than five percent but less than or equal to 10 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact ~~BES Cyber Systems~~BCS, more than 10 percent but less than or equal to 15 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 15 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and

R #	Violation Severity Levels (CIP-002-~~5.1a~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	medium impact ~~BES Cyber Systems~~BCS, five or fewer identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, five percent or fewer high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, five or fewer high or medium ~~BES Cyber Systems~~BCS have not been identified.	incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~and BES Cyber Systems~~BCS, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than five percent but less than or equal to 10 percent high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than five	incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact ~~and BES Cyber Assets~~BCS, more than 10 but less than or equal to 15 identified ~~BES Cyber Assets~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 10 percent but less than or equal to 15 percent high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than 10 but	medium impact ~~BES Cyber Systems~~BCS, more than 15 identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 15 percent of high or medium impact ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact ~~BES Cyber Systems~~BCS have not been identified.

R #	Violation Severity Levels (CIP-002-~~5.1a~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		but less than or equal to 10 high or medium ~~BES Cyber Systems~~BCS have not been identified.	less than or equal to 15 high or medium ~~BES Cyber Systems~~BCS have not been identified.	
R2	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (~~R2~~Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (~~R2~~Part 2.2)	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (~~R2~~Part2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (~~R2~~Part 2.2)	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (~~R2~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (~~R2~~Part 2.2)	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (~~R2~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (~~R2~~Part 2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-002-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
7	TBD	Virtualization Modifications	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High ~~Impact Rating (H)~~impact rating

Each ~~BES Cyber System~~BCS used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium ~~Impact Rating (M)~~impact rating

Each ~~BES Cyber System~~BCS, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each ~~Special Protection System (SPS), Remedial Action Scheme (~~RAS~~),~~ or automated switching System that operates BES Elements, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in ~~High Impact Rating (H)~~high impact rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in ~~High Impact Rating (H),~~high impact rating, above.

2.13. Each Control Center or backup Control Center, not already included in ~~High Impact Rating (H)~~high impact rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low ~~Impact Rating (L)~~impact rating

~~BES Cyber Systems~~BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. ~~Special Protection Systems~~RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.~~

~~For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.~~

~~CIP-002-5.1a~~

~~CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."~~

~~The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber~~

~~Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:~~

~~Dynamic Response to BES conditions~~
~~Balancing Load and Generation~~
~~Controlling Frequency (Real Power)~~
~~Controlling Voltage (Reactive Power)~~
~~Managing Constraints~~
~~Monitoring & Control~~
~~Restoration of BES~~
~~Situational Awareness~~
~~Inter-Entity Real-Time Coordination and Communication~~

~~Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.~~

~~**Entity Registration**~~	~~**RC**~~	~~**BA**~~	~~**TOP**~~	~~**TO**~~	~~**DP**~~	~~**GOP**~~	~~**GO**~~
~~Dynamic Response~~		~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Balancing Load & Generation~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Controlling Frequency~~		~~X~~				~~X~~	~~X~~
~~Controlling Voltage~~			~~X~~	~~X~~	~~X~~		~~X~~
~~Managing Constraints~~	~~X~~		~~X~~			~~X~~	
~~Monitoring and Control~~			~~X~~			~~X~~	
~~Restoration~~			~~X~~			~~X~~	
~~Situation Awareness~~	~~X~~	~~X~~	~~X~~			~~X~~	
~~Inter-Entity coordination~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~	~~X~~

~~**Dynamic Response**~~

~~The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:~~

- ~~Spinning reserves (contingency reserves)~~
    - ~~Providing actual reserve generation when called upon (GO,GOP)~~
    - ~~Monitoring that reserves are sufficient (BA)~~
- ~~Governor Response~~
    - ~~Control system used to actuate governor response (GO)~~
- ~~Protection Systems (transmission & generation)~~
    - ~~Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)~~
    - ~~Zone protection for breaker failure (DP, TO, TOP)~~
    - ~~Breaker protection (DP, TO, TOP)~~
    - ~~Current, frequency, speed, phase (TO,TOP, GO,GOP)~~
- ~~Special Protection Systems or Remedial Action Schemes~~
    - ~~Sensors, relays, and breakers, possibly software (DP, TO, TOP)~~
- ~~Under and Over Frequency relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Under and Over Voltage relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Power System Stabilizers (GO)~~

~~Balancing Load and Generation~~

~~The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:~~

- ~~Calculation of Area Control Error (ACE)~~
    - ~~Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)~~
    - ~~Software used to perform calculation (BA)~~
- ~~Demand Response~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP,DP)~~
- ~~Manually Initiated Load shedding~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP, DP)~~

- ~~Non-spinning reserve (contingency reserve)~~
  - ~~Know generation status, capability, ramp rate, start time (GO, BA)~~
  - ~~Start units and provide energy (GOP)~~

~~Controlling Frequency (Real Power)~~

~~The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:~~

- ~~Generation Control (such as AGC)~~
  - ~~ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)~~
  - ~~Software to calculate unit adjustments (BA)~~
  - ~~Transmit adjustments to individual units (GOP)~~
  - ~~Unit controls implementing adjustments (GOP)~~
- ~~Regulation (regulating reserves)~~
  - ~~Frequency source, schedule (BA)~~
  - ~~Governor control system (GO)~~

~~Controlling Voltage (Reactive Power)~~

~~The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:~~

- ~~Automatic Voltage Regulation (AVR)~~
  - ~~Sensors, stator control system, feedback (GO)~~
- ~~Capacitive resources~~
  - ~~Status, control (manual or auto), feedback (TOP, TO,DP)~~
- ~~Inductive resources (transformer tap changer, or inductors)~~
  - ~~Status, control (manual or auto), feedback (TOP,TO,DP)~~
- ~~Static VAR Compensators (SVC)~~
  - ~~Status, computations, control (manual or auto), feedback (TOP, TO,DP)~~

~~Managing Constraints~~

~~Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:~~

- ~~Available Transfer Capability (ATC) (TOP)~~
- ~~Interchange schedules (TOP, RC)~~
- ~~Generation re-dispatch and unit commit (GOP)~~
- ~~Identify and monitor SOL's & IROL's (TOP, RC)~~
- ~~Identify and monitor Flow gates (TOP, RC)~~

~~Monitoring and Control~~

~~Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:~~

- ~~All methods of operating breakers and switches~~
  - ~~SCADA (TOP, GOP)~~
  - ~~Substation automation (TOP)~~

~~Restoration of BES~~

~~The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:~~

- ~~Restoration including planned cranking path~~
  - ~~Through black start units (TOP, GOP)~~
  - ~~Through tie lines (TOP, GOP)~~
- ~~Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)~~
- ~~Coordination (TOP, TO, BA, RC, DP, GO, GOP)~~

~~Situational Awareness~~

~~The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:~~

- ~~Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)~~
- ~~Change management (TOP,GOP,RC,BA)~~
- ~~Current Day and Next Day planning (TOP)~~
- ~~Contingency Analysis (RC)~~
- ~~Frequency monitoring (BA, RC)~~

~~Inter-Entity Coordination~~

~~The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:~~

- ~~Scheduled interchange (BA,TOP,GOP,RC)~~
- ~~Facility operational data and status (TO, TOP, GO, GOP, RC, BA)~~
- ~~Operational directives (TOP, RC, BA)~~

~~Applicability to Distribution Providers~~

~~It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.~~

~~Requirement R1:~~

~~Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.~~

~~Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.~~

~~Attachment 1~~

~~Overall Application~~

~~In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.~~

- ~~When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.~~
- ~~In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.~~
- ~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.~~

~~High Impact Rating (H)~~

~~This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some~~

~~of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.~~

~~The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.~~

~~Additional thresholds as specified in the criteria apply for this category.~~

~~Medium Impact Rating (M)~~

~~Generation~~

~~The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.~~

- ~~Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.~~

  ~~In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.~~

  ~~By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.~~

~~The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.~~

- ~~In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.~~

  ~~If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.~~

  ~~The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.~~

- ~~Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~

  ~~IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.~~

- ~~Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.~~

- ~~Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.~~

- ~~Criterion 2.13 categorizes as medium impact those BA Control Centers that “control” 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Transmission~~

~~The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist.~~

- ~~Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.~~

- ~~Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.~~

~~It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.~~

- ~~Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:~~

    - ~~Excluded radial facilities that would only provide support for single generation facilities.~~

    - ~~Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.~~

~~The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.~~

~~Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:~~

- ~~230 kV –> 700 MVA~~
- ~~345 kV –> 1,300 MVA~~
- ~~500 kV –> 2,000 MVA~~
- ~~765 kV –> 3,000 MVA~~

~~In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:~~

- ~~For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate~~

~~connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.~~

- ~~Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~
- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

~~Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.~~

1. ~~The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.~~
2. ~~The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.~~

~~The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.~~

- ~~Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~

- ~~Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.~~

- ~~Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.~~

- ~~Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.~~

- ~~Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.~~

  ~~This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.~~

~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.~~

- ~~Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.~~
- ~~Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Low Impact Rating (L)~~

~~BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.~~

~~Restoration Facilities~~

- ~~Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.~~

  ~~In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.~~

  ~~The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.~~

~~Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.~~

~~BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~

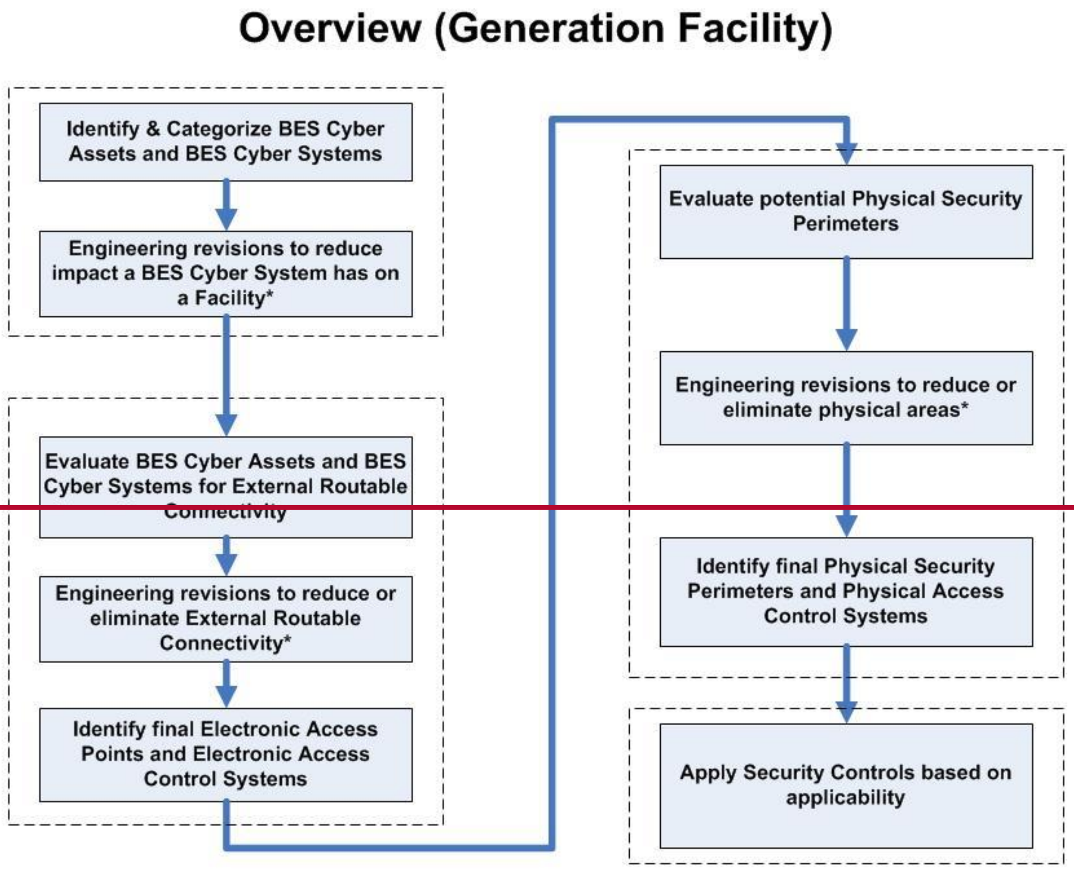
~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.~~

  ~~Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.~~

~~Use Case: CIP Process Flow~~

~~The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.~~



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for R1:~~

~~BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~Rationale for R2:~~

~~The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.~~

~~Version~~	~~Date~~	~~Action~~	~~Change Tracking~~
~~1~~	~~1/16/06~~	~~R3.2 — Change "Control Center" to "control center."~~	~~3/24/06~~
~~2~~	~~9/30/09~~	~~Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.~~ ~~Removal of reasonable business judgment.~~ ~~Replaced the RRO with the RE as a Responsible Entity.~~ ~~Rewording of Effective Date.~~ ~~Changed compliance monitor to Compliance Enforcement Authority.~~	
~~3~~	~~12/16/09~~	~~Updated version number from -2 to -3.~~ ~~Approved by the NERC Board of Trustees.~~	~~Update~~

~~3~~	~~3/31/10~~	~~Approved by FERC.~~	
~~4~~	~~12/30/10~~	~~Modified to add specific criteria for Critical Asset identification.~~	~~Update~~
~~4~~	~~1/24/11~~	~~Approved by the NERC Board of Trustees.~~	~~Update~~
~~5~~	~~11/26/12~~	~~Adopted by the NERC Board of Trustees.~~	~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.~~
~~5.1~~	~~9/30/13~~	~~Replaced "Devices" with "Systems" in a definition in background section.~~	~~Errata~~
~~5.1~~	~~11/22/13~~	~~FERC Order issued approving CIP-002-5.1.~~	
~~5.1a~~	~~11/02/16~~	~~Adopted by the NERC Board of Trustees.~~	
~~5.1a~~	~~12/14/2016~~	~~FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.~~	

~~Appendix 1~~

~~**Requirement Number and Text of Requirement**~~
~~CIP-002-5.1, Requirement R1~~ ~~R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:~~ ~~i. Control Centers and backup Control Centers;~~ ~~ii. Transmission stations and substations;~~ ~~iii. Generation resources;~~ ~~iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;~~ ~~v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and~~ ~~vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.~~ ~~1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;~~ ~~1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and~~ ~~1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).~~ ~~Attachment 1, Criterion 2.1~~ ~~2. Medium Impact Rating (M)~~ ~~Each BES Cyber System, not included in Section 1 above, associated with any of the following:~~ ~~2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~
~~**Questions**~~
~~Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."~~ ~~The Interpretation Drafting Team identified the following questions in the RFI:~~

1. ~~Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~
2. ~~Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~
3. ~~If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~Responses~~

~~Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~

~~The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)~~

~~Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:~~

> ~~The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~

~~The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.~~

~~The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:~~

> ~~Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating~~

~~criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1:~~ **~~Impact Rating of Generation Resource Shared BES Cyber Systems~~** ~~for further information and examples.~~

~~Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~The phrase applies to each discrete BES Cyber System.~~

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-2

Proposed Reliability Standard CIP-003-10
Clean

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-10

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1. Balancing Authority

      4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

            4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

      4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-10:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that

include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with mandatory and enforceable Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	within 18 calendar months of the previous approval. (R1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote	

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)	access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-003-10 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	TBD	Virtualization Modifications	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process

documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - security information management logging alerts;
    - time-of-need session initiation;
    - session recording;
    - system logs; or
    - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
    - disabling vendor electronic remote access user or system accounts;
    - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
    - disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;

  - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
  - administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
  - other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
   - Anti-malware technologies;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Automated or manual log reviews;
   - alerting; or
   - other operational, procedural, or technical controls.

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-2

Proposed Reliability Standard CIP-003-10
Redline

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-10~~9~~

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-~~9~~10:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (~~ESPs~~ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~3.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~3.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan~~ for CIP-003-9.~~."

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact ~~BES Cyber Systems~~BCS, if any:

1.1.1. Personnel and training (CIP~~-~~-004);

1.1.2. Electronic Security Perimeters (CIP~~-~~-005) including Interactive Remote Access;

1.1.3. Physical security of ~~BES Cyber Systems~~BCS (CIP~~-~~-006);

1.1.4. System security management (CIP~~-~~-007);

1.1.5. Incident reporting and response planning (CIP~~-~~-008);

1.1.6. Recovery plans for ~~BES Cyber Systems~~BCS (CIP~~-~~-009);

1.1.7. Configuration change management and vulnerability assessments (CIP~~-~~-010);

1.1.8. Information protection (CIP~~-~~-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP~~-~~-002 containing low impact ~~BES Cyber Systems~~BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP~~-~~-002 containing low impact ~~BES Cyber Systems~~BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* ~~*[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*~~

Note: An inventory, list, or discrete identification of low impact ~~BES Cyber Systems~~BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2.~~-~~_Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3.~~-~~_An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4.~~-~~_An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with ~~the NERC~~mandatory and enforceable Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non~~-~~-compliant, it shall keep information related to the non~~-~~-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records~~,~~ and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address one of the nine topics required by Requirement R1. (~~R1~~Part1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part~~R~~1.1)	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R1~~Part1.1) OR The Responsible Entity did not complete its approval of the one or more documented	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address three of the nine topics required by Requirement R1. (Part ~~R~~1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (~~R1~~Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address four or more of the nine topics required by Requirement R1. (Part~~R~~1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1. (Part~~R~~1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-003-~~9~~10)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>OR
The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part~~R~~1.1)
OR
The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS~~BES Cyber Systems~~, but did not address one of the seven topics required by Requirement R1. (Part~~R~~1.2)
OR</td><td>cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part~~R~~1.1)
OR
The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address two of the seven topics required by Requirement R1. (Part~~R~~1.2)
OR
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 16</td><td>cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1)
OR
The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address three of the seven topics required by Requirement R1. (Part~~R~~1.2)
OR
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required</td><td>previous review. (Requirement R1)
OR
The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by ~~R1~~Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part~~R~~1.1)
OR
The Responsible Entity ~~documented one or more cyber security policies for its assets identified in CIP-002 containing low impact~~ ~~BES Cyber Systems, but~~ did not address four or more of the seven topics required by Requirement R1. (Part~~R~~1.2)
OR
The Responsible Entity did not have any documented cyber</td></tr>
</table>

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~BES Cyber Systems~~ as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or	calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R1~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part ~~R~~1.2)	by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part~~R~~1.2)	security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1. (Part~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part~~R~~1.2)

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	equal to 16 calendar months of the previous approval. (~~R1~~Part 1.2)			
R2	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~implemented electronic access controls but~~ failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber~~	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber~~	The Responsible Entity ~~documented the physical access controls for its assets containing low impact BES Cyber Systems, but~~ failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but~~ failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR	The Responsible Entity failed to document and implement one or more cyber security plan(s) ~~for its assets containing low impact BES Cyber Systems~~ according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for~~	~~security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls but~~ failed to implement authentication for all Dial-up Connectivity ~~that provides access to low impact BES Cyber System(s), per Cyber Asset capability~~ according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity ~~documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES~~	The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but~~ failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR	

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Transient Cyber Assets and Removable Media, but~~ failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets, but~~ failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	~~Cyber Systems, but~~ failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for Transient Cyber Asset managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR	

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		~~Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Asset managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)		
R3	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has~~ did not identify~~ied~~, by name, a CIP Senior Manager. OR The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has used delegated authority for actions where allowed by the CIP Standards, but~~ does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-003-10 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026

10	TBD	Modified by Project 2016-02	

Attachment 1

Required Sections for Cyber Security Plan(s)~~ for Assets Containing Low Impact BES Cyber Systems~~

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple~~-~~-impact ~~BES Cyber Systems~~BCS ratings can utilize policies, procedures, and processes for their high or medium impact ~~BES Cyber Systems~~BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. ~~Section 1.~~ Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. ~~Section 2.~~ Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset, and (2) the Cyber Asset(s~~),~~) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. ~~Section 3.~~ Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP~~-~~-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. ~~between~~Between:

- a low impact ~~BES Cyber System(s)~~ BCS; or
- An SCI that supports a low impact BCS

and a Cyber ~~Asset~~System(s) outside the asset containing~~ low impact BES Cyber System(s);~~:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

~~i.~~ii. using a routable protocol when entering or leaving the asset containing the low impact ~~BES Cyber System(s);~~BCS or SCI that supports a low impact BCS; and

~~ii.~~iii. not used for time~~-~~-sensitive ~~protection or control functions between intelligent electronic devices (e.g.,~~ communications ~~using protocol IEC TR-61850-90-5 R-GOOSE).~~of Protection Systems.

3.2 Authenticate all Dial~~-~~-up Connectivity, if any, that provides access to low impact ~~BES Cyber System(s),~~BCS or SCI that supports a low impact BCS, per ~~Cyber Asset~~system capability.

Section 4. ~~**Section 4.**~~ Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E~~-~~-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. ~~Transient Cyber Asset~~ TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact ~~BES Cyber Systems~~BCS, through the use of ~~Transient Cyber Assets~~TCA or Removable Media. The plan(s) shall include:

5.1 For ~~Transient Cyber Asset(s)~~TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on~~-~~-demand manner (per ~~Transient Cyber Asset~~TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting ~~the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset~~(per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- ~~Other~~Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset.~~TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a ~~BES Cyber System~~BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~BCS or SCI that supports a low impact BCS.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) ~~for Assets Containing Low Impact BES Cyber Systems~~

Section 1. ~~Section 1.~~ Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e~~-~~-mails, memos, or computer~~-~~-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. ~~Section 2.~~ Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset; and
  b. The Cyber ~~Asset~~System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. ~~Section 3.~~ Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets~~ containing low impact BES Cyber Systems, ~~, the routable protocol communication ~~between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset~~as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that ~~communication is~~communications are used for time~~-~~-sensitive ~~protection or control functions between intelligent electronic devices~~communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) ~~between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s)~~ or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial~~-~~-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial~~-~~-back modems, modems that must be remotely controlled by the control center or control room, or access control on the ~~BES Cyber System~~BCS).

Section 4. ~~Section 4.~~ Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E~~-~~-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. ~~Section 5.~~ ~~Transient Cyber Asset~~TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

~~1.~~ Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of ~~live operating systems or~~ system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

2. identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

   Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code~~.~~

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
   - steps to preauthorize access;
   - alerts generated by vendor log on;
   - session monitoring;
   - security information management logging alerts;
   - time-of-need session initiation;
   - session recording;
   - system logs; or
   - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
   - disabling vendor electronic remote access user or system accounts;

- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
- disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - alerting; or
    - other operational, procedural, or technical controls.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-3

Proposed Reliability Standard CIP-004-8
Clean

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-8
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.
4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. **Balancing Authority**

4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. **Generator Operator**

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part.	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.
2.2	High impact BCS and their associated:	Require completion of the training	Examples of evidence may include, but are

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
	SCI supporting an Applicable System in this Part	If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part		
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP) (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access (except for medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts; and authorized unescorted physical access (except for medium impact BCS without ERC) that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Examples of evidence may include, but are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High impact BCS and their associated	For termination actions, revoke the	Examples of evidence may include, but are

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	EACMS SCI supporting an Applicable System in this Part	individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	authorized unescorted physical access. (Part 2.2) OR The Responsible Entity did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for two individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1)	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)
R5	The Responsible Entity did not revoke individual’s user accounts upon termination action within 30 calendar days of the date of	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	termination action for one or more individuals. (Part 5.3) OR The Responsible Entity did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	within 24 hours of the termination action for one individual. (Part 5.1) OR The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	complete the removal within 24 hours of the termination action for two individuals. (Part 5.1) OR The Responsible Entity for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action for three or more individuals. (Part 5.1) OR The Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (Requirement R6) OR The Responsible Entity, for four or more individuals, did not authorize provisioned electronic access to

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	The Responsible Entity did not perform the verification required by Part 6.2 within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for one individual, did not remove the individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for two individuals, did remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for three individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for four or more individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-004-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
8	TBD	Virtualization Modifications	

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-3
Proposed Reliability Standard CIP-004-8
Redline

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-~~7~~8

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting ~~BES Cyber Systems~~BCS.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. **Balancing Authority**

4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. **Generator Operator**

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~7~~8:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002~~-5.1a~~ identification and categorization processes.

~~5. **Effective Dates:** See Implementation Plan for CIP-004-7.~~

~~6. **Background:** Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards~~

~~include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~” Columns in Tables:~~

~~6.1.~~4.3. ”: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies. ~~The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.~~

- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity –** Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS) –** Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

5. Effective Dates: See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~7~~8 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES~~impact BCS Medium impact BCS Shared Cyber ~~Systems~~Infrastructure (SCI) supporting an Applicable System in this Part. ~~Medium Impact BES Cyber Systems~~	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to ~~BES Cyber~~Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. -Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~7~~8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~7~~8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~7~~8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS~~;~~); and ~~2. PACS~~ 2. Physical Access Control Systems (PACS) Medium ~~Impact BES Cyber Systems~~ impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for ~~BES Cyber Systems~~BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a ~~BES Cyber System's~~BCS electronic interconnectivity and interoperability with other Cyber ~~Assets~~Systems, including Transient Cyber Assets~~,~~ (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~7~~8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to ~~applicable Cyber Assets~~Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

CIP-004-~~7~~8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Part		

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to ~~BES Cyber~~Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber~~	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of the Responsible Entity's

CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
	2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	conducted according to Parts 3.1 through 3.3.	criteria or process for verifying contractors or service vendors personnel risk assessments.
3.5	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 ~~to~~through 3.4 within the last seven years.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~7~~8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP) (except for medium impact BCS without ERC).	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a ~~Physical Security Perimeter.~~PSP.
4.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated:	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or

CIP-004-~~7~~8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part		- Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~7~~8 Table R5 – ~~-~~Access Revocation

Part	Applicable Systems	Requirements	Measures
5.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access (except for medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated:	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts; and authorized unescorted physical access (except for medium impact BCS without ERC) that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible

CIP-004-~~7~~8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part		Entity determines is not necessary.
5.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the ~~“~~Applicable Systems~~”~~ identified in *CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1~~.)~~) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI~~.~~ (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.

CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. ~~C.~~ Compliance

1. **Compliance Monitoring Process:**

1.1. **Compliance Enforcement Authority:** "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance.~~ ~~For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. ~~(~~(Part 2.1) OR

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. ~~(~~(Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting authorized electronic or authorized unescorted	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting authorized electronic or	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing ~~Personnel Risk Assessments (PRAs),~~personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	access for one individual. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR	physical access for two individuals. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~through 3.2.2 for two individuals. (Parts 3.2 & 3.4)	authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~through 3.2.2 for	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)	OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)	three individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 ~~&~~through 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)	not include the required checks described in 3.2.1 ~~and~~through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR ~~The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 ~~&~~through 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for 5% or less of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. ~~(~~(Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 5% but less than (or equal to) 10% of its ~~BES Cyber~~	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 10% but less than (or equal to) 15% of its ~~BES~~	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR The Responsible Entity did not ~~implement one or more documented program(s) for access management that includes a process to~~ authorize electronic access or unescorted physical access~~. (~~ based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. ~~(~~(Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		~~Systems~~BCS or SCI, privileges were incorrect or unnecessary. ~~(~~(Part 4.3)	~~Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	verification ~~but~~ for more than 15% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. ~~(~~(Part 4.3)
R5	The Responsible Entity ~~has implemented one or more process(es) to~~ did not revoke ~~the~~ individual's user accounts upon termination action ~~but did not do so for~~ within 30 calendar days of the date of termination action for one or more individuals. (Part 5.3) OR The Responsible Entity ~~has implemented one or more process(es) to~~did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer~~, but did not do so for~~ within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR	The Responsible Entity ~~has implemented one or more process(es) to remove the~~ did not initiate removal of the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for one individual. (Part 5.1) OR ~~The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by	The Responsible Entity ~~has implemented one or more process(es) to remove the~~ did not initiate removal of the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for two individuals. (Part 5.1) OR ~~The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~The Responsible Entity for two individuals, did not revoke the authorized	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity ~~has implemented one or more process(es) to remove~~did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for three or more individuals. (Part 5.1) OR ~~The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~The

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but~~The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	the end of the next calendar day following the predetermined date. (Part 5.2)	electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity~~ has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. ~~(~~(Part 6.1) OR The Responsible Entity ~~performed~~did not perform the verification required by ~~Requirement R6~~ Part 6.2 ~~more~~	The Responsible Entity~~ has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. ~~(~~(Part 6.1) OR The Responsible Entity ~~performed~~did not perform the verification required by	The Responsible Entity~~ has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. ~~(~~(Part 6.1) OR The Responsible Entity ~~performed~~did not perform the verification required by	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. ~~(~~(Requirement R6) OR The Responsible Entity~~ has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. ~~(~~(Part 6.1)

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~than~~within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. ~~(~~(Part 6.2) OR The Responsible Entity ~~has implemented~~, for one ~~or more program(s) to~~individual, did not remove the individual's ability to use provisioned access to BCSI ~~but, for one individual, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	~~Requirement R6~~ Part 6.2 ~~more than~~within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. ~~(~~(Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to~~, for two individuals, did remove ~~the~~each individual's ability to use provisioned access to BCSI ~~but, for two individuals, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	~~Requirement R6~~ Part 6.2 ~~more than~~within 17 calendar months but less than or equal to 18 calendar months of the previous verification. ~~(~~(Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to~~, for three individuals, did not remove ~~the~~each individual's ability to use provisioned access to BCSI ~~but, for three individuals, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	OR The Responsible Entity ~~performed~~did not perform the verification required by ~~Requirement R6~~ Part 6.2 more than 18 calendar months of the previous verification. ~~(~~(Part 6.2) OR The Responsible Entity ~~has implemented one~~, for four or more ~~program(s) to~~individuals, did not remove ~~the~~each individual's ability to use provisioned access to BCSI ~~but, for four or more individuals, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- ~~None.~~Implementation Plan for Project 2016-02
- CIP-004-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
~~7~~8	~~12/7/21~~TBD	~~FERC Order issued approving CIP-004-7~~ ~~Docket No. RD21-6-000~~Modified by Project 2016-02.	
~~7~~	~~12/10/21~~	~~Effective Date~~	~~1/1/24~~

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-4

Proposed Reliability Standard CIP-005-8
Clean

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-8

3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP.	Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Systems connected via a routable protocol within each ESP.
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that control an ESP for an Applicable System in Part 1.1	Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.	Examples of evidence may include, but are not limited to, documentation of the methods implemented to permit only needed network accessibility to Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the Management Interfaces (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).
1.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious routable protocol communications detection methods (e.g., intrusion detection system, application layer firewall, etc.) are implemented.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.6	High impact BCS and their associated PCA Medium impact BCS at Control Centers and their associated PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time-sensitive communication of Protection Systems.	Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Permit Interactive Remote Access (IRA), if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	Intermediate System(s) used to access an Applicable System in Part 2.1	Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Examples of evidence may include, but are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption) initiate and terminate.
2.3	Intermediate System(s) used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Example of evidence may include, but are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID;

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
2.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, including IRA and system-to-system remote access, such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g., connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g., netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High impact BCS and their associated PCA	Have one or more method(s) to	Examples of evidence may include,

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	disable active vendor remote access (including IRA and system-to-system remote access).	but are not limited to, documentation of the methods(s) used to disable active vendor remote access • (including IRA and system-to-system remote access).
2.6	Intermediate System(s) used to access an Applicable System in Part 2.1	Prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System and supporting Cyber Systems.
2.7	Intermediate System(s) used to access an Applicable System in Part 2.1	Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Network diagrams of Intermediate Systems architecture; or • Configuration, settings, or policy of the EAP which controls routable protocol communications of IRA through the ESP.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part .	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part.	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority:** "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious routable protocol communications entering or leaving the ESP required by Part 1.5. OR The Responsible Entity did not document the reason for permitting communications. (Part 1.2)	The Responsible Entity did not document one or more processes for CIP-005-8 Table R1 – Electronic Security Perimeter. (R1) OR The Responsible Entity did not protect the Applicable Systems connected to the network with routable protocol with an ESP. (Part 1.1) OR The Responsible Entity did not permit only needed communications and deny all other communications, through the ESP; excluding time sensitive communications of Protection Systems. (Part 1.2) OR The Responsible Entity did not protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces for Applicable

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Systems per system capability. (Part 1.3) OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the Applicable Systems. (Part 1.4) OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to span a single ESP between PSPs, as required by Part 1.6.
R2.	The Responsible Entity does not have documented processes for one or more of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable Requirement Parts 2.1 through 2.3. OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access	The Responsible Entity did not implement processes for three of the applicable Requirement Parts 2.1 through 2.3. OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote access

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(including IRA and system-to-system remote access) (Part 2.5).	(including IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not prevent Intermediate System(s) from sharing CPU resources or memory resources with any part of a high or medium impact BCS or associated PCAs. (Part 2.6). OR The Responsible Entity did not ensure routable protocol communications from an Intermediate System to high or medium impact BCS or associated PCAs went through an ESP (Part 2.7).
R3.	The Responsible Entity did not document one or more processes for CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI. (Requirement R3)	The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.1). OR	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity did not have a method to determine authenticated vendor-initiated	The Responsible Entity did not implement any processes for CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI. (Requirement R3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.2).	remote connections for EACMS or SCI supporting EACMS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS or SCI supporting EACMS (Part 3.2).	The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
7	11/05/2020	Adopted by the NERC Board of Trustees.	
7	03/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
7	4/5/2021	Effective Date	10/1/2022
8	TBD	Virtualization Modifications	

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-4
Proposed Reliability Standard CIP-005-8
Redline

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-~~7~~8

3. **Purpose:** To ~~manage electronic access to~~protect BES Cyber Systems (BCS) against compromise by ~~specifying a~~permitting only known and controlled ~~Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to~~communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-~~7~~8:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~**4.2.3.2.**~~**4.2.3.3.** Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems”: Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”~~Implementation Plan for Project 2019-03.~~

~~6.~~ ~~**Background:**~~ ~~Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with,~~ ~~*“Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].”*~~ ~~The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term~~ ~~*documented processes*~~ ~~refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms~~ ~~*program*~~ ~~and~~ ~~*plan*~~ ~~are sometimes used in place of~~ ~~*documented processes*~~ ~~where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as~~ ~~*plans*~~ ~~(i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single trainingprogram could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~
- ~~**High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.~~

- ~~**High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~
- ~~**Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA	~~All applicable Cyber Assets~~Applicable Systems connected to a network via a routable protocol ~~shall reside within a defined~~must be protected by an ESP.	~~An example~~Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber ~~Assets~~Systems connected via a routable protocol within each ESP.
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
			configuration).
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that control an ESP for an Applicable System in Part 1.1	Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.	Examples of evidence may include, but are not limited to, documentation of the methods implemented to permit only needed network accessibility to Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the Management Interfaces (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).
1.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious routable protocol communications detection methods (e.g., intrusion detection system, application

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
			layer firewall, etc.) are implemented.
1.~~2~~6	High ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS at Control Centers and their associated~~:~~ PCA	~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ~~i.~~ii. Time-sensitive communication of Protection Systems.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, ~~network diagrams showing all external routable communication paths~~documentation of methods used to protect the confidentiality and integrity of the ~~identified EAPs.~~ data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

~~CIP-005-7 Table R1 – Electronic Security Perimeter~~

~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~

~~1.3~~	~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	~~Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.~~	~~An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.~~
~~1.4~~	~~High Impact BES Cyber Systems with Dial-up Connectivity and their associated:~~ - ~~PCA~~ ~~Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated:~~ - ~~PCA~~	~~Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.~~	~~An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.~~
~~1.5~~	~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers~~	~~Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.~~	~~An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.~~

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, ~~where technically feasible~~per system capability, in *CIP-005-~~7~~8 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~7~~8 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS and their associated~~:~~ PCA SCI supporting an Applicable System in this Part	~~For all~~Permit Interactive Remote Access~~,~~ ~~utilize~~ (IRA), if any, only through an Intermediate System~~ such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~.	Examples of evidence may include, but are not limited to, network diagrams~~ or~~, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~Intermediate System(s) used to access an Applicable System in Part 2.1	~~For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.~~Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption ~~initiates~~) initiate and ~~terminates.~~ terminate.

CIP-005-~~7~~8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~• PCA~~ Intermediate System(s) used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for ~~all~~ ~~Interactive Remote Access sessions~~IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	~~An example~~Example of evidence may include, but ~~is~~are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
2.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ ~~•~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~ impact BCS and their associated~~:~~ ~~•~~ PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, ~~(~~including ~~Interactive Remote Access~~ IRA and system-to-system remote access~~),~~ , such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions;

CIP-005-~~7~~8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			- Methods for monitoring activity (e.g~~.~~., connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g~~.~~., netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or - Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~ impact BCS and their associated~~:~~ PCA SCI supporting an Applicable System in this Part	Have one or more method(s) to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including ~~Interactive Remote Access~~ IRA and system-to-system remote access~~),~~ ~~such as:~~ - ~~Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or~~ - ~~Methods to disable vendor Interactive Remote Access at~~

CIP-005-~~7~~8 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
			~~the applicable Intermediate System.~~).
2.6	Intermediate System(s) used to access an Applicable System in Part 2.1	Prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System and supporting Cyber Systems.
2.7	Intermediate System(s) used to access an Applicable System in Part 2.1	Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Network diagrams of Intermediate Systems architecture; or • Configuration, settings, or policy of the EAP which controls routable protocol communications of IRA through the ESP.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-~~7~~8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and ~~PACS~~SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*.

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS~~SCI

Part	Applicable Systems	Requirements	Measures
3.1	EACMS and PACS associated with ~~High Impact BES Cyber Systems~~ high impact BCS. EACMS and PACS associated with ~~Medium Impact BES Cyber Systems~~medium impact BCS with ~~External Routable Connectivity~~ ERC. SCI supporting an Applicable System in this Part .	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with ~~High Impact BES Cyber Systems~~high impact BCS. EACMS and PACS associated with ~~Medium Impact BES Cyber Systems~~medium impact BCS with ~~External Routable Connectivity~~ ERC. SCI supporting an Applicable System in this Part.	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a

CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS~~SCI

Part	Applicable Systems	Requirements	Measures
			firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious routable protocol communications entering or leaving the ESP required by Part 1.5. OR The Responsible Entity did not document the reason for ~~both inbound and outbound~~permitting communications. (Part 1.~~5)~~2)	The Responsible Entity did not document one or more processes for *CIP-005-~~6~~8 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not ~~have all applicable Cyber Assets~~protect the Applicable Systems connected to ~~a~~the network ~~via a~~with routable protocol ~~within a defined Electronic Security Perimeter (ESP). (~~with an ESP. (Part 1.1) OR ~~External Routable Connectivity through the ESP was not through an identified EAP. (1.2)~~ ~~OR~~ The Responsible Entity did not ~~require inbound and outbound access permissions~~permit only needed communications and deny all other

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~access~~communications, through the ESP; excluding time sensitive communications of Protection Systems. (Part 1.2) OR The Responsible Entity did not protect ESP and SCI configurations by ~~default.~~ ~~(~~implementing methods to permit only needed network accessibility to Management Interfaces for Applicable Systems per system capability. (Part 1.3) OR The Responsible Entity did not perform authentication when establishing ~~dial~~Dial-up ~~connectivity with the applicable Cyber Assets, where technically feasible.~~ ~~(~~Connectivity with the Applicable Systems. (Part 1.4) OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				span a single ESP between PSPs, as required by Part 1.6.
R2.	The Responsible Entity does not have documented processes for one or more of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5).	The Responsible Entity did not implement processes for three of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~ IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not prevent Intermediate System(s) from sharing CPU resources or memory resources with any part of

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				a high or medium impact BCS or associated PCAs. (Part 2.6). OR The Responsible Entity did not ensure routable protocol communications from an Intermediate System to high or medium impact BCS or associated PCAs went through an ESP (Part 2.7).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS.~~ ~~(~~SCI.* (Requirement R3)	The Responsible Entity ~~had method(s) as required by Part 3.1 for EACMS but~~ did not have a method to determine authenticated vendor-initiated remote connections for PACS ~~(~~or SCI supporting PACS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for EACMS but~~ did not have a method to terminate authenticated vendor-initiated remote connections for PACS ~~(3.2~~or SCI supporting PACS (Part 3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity ~~had method(s) as required by Part 3.1 for PACS but~~ did not have a method to determine authenticated vendor-initiated remote connections for EACMS ~~(~~or SCI supporting EACMS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for PACS but~~ did not	The Responsible Entity did not implement any processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS.~~ ~~(~~SCI.* (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS ~~(~~or SCI supporting EACMS (Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-005-~~7~~8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
7	11/05/2020	Adopted by the NERC Board of Trustees.	
7	~~3~~03/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
7	4/5/2021	Effective Date	10/1/2022
8	TBD	Virtualization Modifications	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-5

Proposed Reliability Standard CIP-006-7
Clean

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific Requirement Part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.1	Medium impact BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium impact BCS with ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access, per system capability.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Monitor for unauthorized access through a physical access point into a PSP.	Examples of evidence may include, but are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a PSP.
1.5	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a PSP and additional evidence that the alarm or alert was issued and communicated as identified in the Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Monitor each PACS for unauthorized physical access to a PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	PACS associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.
1.8	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each PSP, with information to identify the individual and date and time of entry.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes logging and recording of physical entry into each PSP and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each PSP that show the individual and the date and time of entry into each PSP.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days.	Examples of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP that show the date and time of entry into each PSP.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.1	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each PSP.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require manual or automated logging of visitor entry into and exit from each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain visitor logs for at least 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	PACS associated with: • High impact BCS, or • Medium impact BCS with ERC Locally mounted hardware or devices at the PSP associated with: • High impact BCS, or • Medium impact BCS with ERC	Maintenance and testing of each PACS and locally mounted hardware or devices at each PSP at least once every 24 calendar months to ensure they function properly.	Examples of evidence may include, but are not limited to, a maintenance and testing program that provides for testing each PACS and locally mounted hardware or devices associated with each applicable each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. **Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Assessment Processes:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Part 1.3) OR The Responsible Entity does not have a process to monitor

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				for unauthorized access through a physical access point into a PSP. (Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each PACS for unauthorized physical access to a PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				authorized physical entry into each PSP with sufficient information to identify the individual and date and time of entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				visitor control program to retain visitor logs for at least 90 days. (Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for PACS and locally mounted hardware or devices at the PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for PACS and locally mounted hardware or devices at the PSP, but did not complete required testing within 27 calendar months. (Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-006-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-5

Proposed Reliability Standard CIP-006-7
Redline

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-~~6~~7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~**4.1.6**~~**4.1.5 Reliability Coordinator**

~~**4.1.7**~~**4.1.6 Transmission Operator**

~~**4.1.8**~~**4.1.7 Transmission Owner**

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-~~6~~7:

4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5.1~~ identification and categorization processes.

~~5. Effective Dates:~~

~~See Implementation Plan for CIP-006-6.~~

~~6. Background:~~

~~Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the~~

~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~**” Columns in Tables:**~~

4.3. **”:** Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific ~~requirement row~~Requirement Part applies. ~~The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

- ~~**Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

5. ~~**Locally mounted hardware or devices at the Physical Security Perimeter** – Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

Effective Dates: See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-~~6~~7 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-~~6~~7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-~~6~~7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.1	Medium ~~I~~impact ~~BES cyber Systems~~ BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High i~~I~~mpact ~~BES Cyber Systems~~BCS, or • Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	~~An example~~Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.

CIP-006-~~6~~7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable ~~Physical Security Perimeter~~PSP to only those individuals who have authorized unescorted physical access.	~~An example~~Examples of evidence may include, but are not limited to, language in the physical security plan that describes each ~~Physical Security Perimeter~~PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA -SCI supporting an Applicable System in this Part	~~Where technically feasible, utilize~~Utilize two or more different physical access controls (this does not require two completely independent ~~physical access control systems~~PACS) to collectively allow unescorted physical access into ~~Physical Security Perimeters~~PSPs to only those individuals who have authorized unescorted physical access~~.~~ , per system capability.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, language in the physical security plan that describes ~~the Physical Security Perimeters~~each PSP and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-~~6~~7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.4	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~ PSP.	Examples ~~An example~~ of evidence may include, but are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~ PSP.
1.5	High i~~I~~mpact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~ PSP to the personnel identified in the ~~BES~~ Cyber Security Incident response plan within 15 minutes of detection.	Examples ~~An example~~ of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a ~~Physical Security Perimeter~~ PSP and additional evidence that the alarm or alert was issued and communicated as identified in the ~~BES~~ Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

CIP-006-~~6~~7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.6	Physical Access Control Systems (PACS) associated with: • High i~~I~~mpact ~~BES Cyber Systems~~ BCS, or • Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC SCI supporting an Applicable System in this Part	Monitor each ~~Physical Access Control System~~ PACS for unauthorized physical access to a ~~Physical Access Control System~~ PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.
1.7	~~Physical Access Control Systems (~~PACS~~)~~ associated with: • High i~~I~~mpact ~~BES Cyber Systems~~BCS, or • Medium i~~I~~mpact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized physical access to a ~~Physical Access Control System~~ PACS to the personnel identified in the ~~BES~~ Cyber Security Incident response plan within 15 minutes of the detection.	Examples ~~An example~~ of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to ~~Physical Access Control Systems~~ PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-~~6~~7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.8	High i~~I~~mpact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each ~~Physical Security Perimeter~~PSP, with information to identify the individual and date and time of entry.	Examples ~~An example~~ of evidence may include, but are not limited to, language in the physical security plan that describes logging and recording of physical entry into each PSP ~~Physical Security Perimeter~~ and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each PSP ~~Physical Security Perimeter~~ that show the individual and the date and time of entry into each PSP ~~Physical Security Perimeter~~.
1.9	High i~~I~~mpact BCS ~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact BCS ~~BES Cyber Systems~~ with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP ~~Physical Security Perimeter~~ for at least 90 calendar days.	Examples ~~An example~~ of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP ~~Physical Security Perimeter~~ that show the date and time of entry into each PSP~~Physical Security Perimeter~~.

~~1.10~~	~~High Impact BES Cyber Systems and their associated:~~ - ~~PCA~~ ~~Medium Impact BES Cyber Systems at Control Centers and their associated:~~ ~~PCA~~	~~Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.~~ ~~Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:~~ - ~~encryption of data that transits such cabling and components; or~~ - ~~monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or~~ - ~~an equally effective logical protection.~~	~~An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.~~

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-~~6~~7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-~~6~~7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~6~~7 Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each ~~Physical Security Perimeter, except during CIP Exceptional Circumstances.~~PSP.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, language in a visitor control program that requires continuous escorted access of visitors within ~~Physical Security Perimeters~~each PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.
2.2	High i~~I~~mpact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from each ~~Physical Security Perimeter~~ PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor~~, except during CIP Exceptional Circumstances~~.	Examples ~~An example~~ of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each ~~Physical Security Perimeter~~ PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

	SCI supporting an Applicable System in this Part		

CIP-006-~~6~~7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain visitor logs for at least 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-~~6~~7 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-~~6~~7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~6~~7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	~~Physical Access Control Systems (~~PACS~~)~~ associated with: • High ~~Impact BES Cyber Systems~~impact BCS, or • Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC Locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP associated with: • High ~~Impact BES Cyber Systems~~impact BCS, or • Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC	Maintenance and testing of each ~~Physical Access Control System~~PACS and locally mounted hardware or devices at ~~the Physical Security Perimeter~~each PSP at least once every 24 calendar months to ensure they function properly.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, a maintenance and testing program that provides for testing each ~~Physical Access Control System~~PACS and locally mounted hardware or devices associated with each applicable ~~Physical Security Perimeter~~each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. **Compliance Monitoring Process:**

~~1.1.~~ Compliance Enforcement Authority:

~~1.2.~~1.1. As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

~~1.3.~~ Evidence Retention:

1.2. The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

~~1.4.~~ Compliance Monitoring and Assessment Processes:

~~1.5.~~1.3. As defined in the NERC Rules of Procedure, "Compliance ~~Audits~~Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.6. Additional Compliance Information:~~

~~None~~

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Part 1.3) OR

R #	Violation Severity Levels (CIP-006-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter. (~~PSP. (Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each ~~Physical Access Control System~~PACS for unauthorized physical access to a ~~Physical Access Control Systems. (~~PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for

R #	Violation Severity Levels (CIP-006-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				unauthorized physical access to ~~Physical Access Control Systems~~PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each ~~Physical Security Perimeter~~PSP with sufficient information to identify the individual and date and time of entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9) ~~OR~~ ~~The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical~~

R #	Violation Severity Levels (CIP-006-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)~~
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the

R #	**Violation Severity Levels (CIP-006-~~6~~7)**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ~~ninety~~90 days. (Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter. (~~PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-006-~~6~~7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td></td><td>testing within 27 calendar months. (Part 3.1)</td></tr>
</table>

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~

- Implementation Plan for Project 2016-02
- CIP-006-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~General:~~

~~While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.~~

~~Requirement R1:~~

~~Methods of physical access control include:~~

- ~~Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~
- ~~Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~
- ~~Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~

- ~~Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.~~

~~Methods to monitor physical access include:~~

- ~~Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.~~
- ~~Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.~~

~~Methods to log physical access include:~~

- ~~Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.~~
- ~~Video Recording: Electronic capture of video images of sufficient quality to determine identity.~~
- ~~Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.~~

~~The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.~~

~~Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.~~

~~The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the~~

~~physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.~~

~~This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.~~

~~The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.~~

~~The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an "an equally effective logical protection" in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.~~

~~The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity's BES Cyber Systems while not requiring controls to be~~

~~implemented on third-party components when entities rely on leased third-party communications.~~

~~In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.~~

~~Requirement R2:~~

~~The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.~~

~~The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.~~

~~Requirement R3:~~

~~This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.~~

~~Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable~~

~~communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.~~

~~Rationale for Requirement R2:~~

~~To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.~~

~~Rationale for Requirement R3:~~

~~To ensure all Physical Access Control Systems and devices continue to function properly.~~

Exhibit A-6

Proposed Reliability Standard CIP-007-7
Clean

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002- identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See Project 2016-02 Modifications to CIP Standards Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports or network accessible logical services, individually or by group; • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; • Configuration or settings of host-based firewalls or other device level mechanisms that disable or prevent unneeded network accessible logical ports or network accessible logical services; or • Identity or process based access policy or workload configuration demonstrating needed network accessibility.

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium impact BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Examples of evidence may include, but are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting either: High impact BCS or their associated PCA. Medium impact BCS or their associated PCA.	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Cyber Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.	Examples of evidence may include, but are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.
2.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Examples of evidence may include, but are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security patches released by the documented sources at least once every 35 calendar days.
2.3	High impact BES Cyber Systems and their	For applicable patches identified in Part	Examples of evidence may include, but

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	are not limited to: - Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of component software revision, or registry exports that show software has been installed); or - A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.
2.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Examples of evidence may include, but are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Prevention

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of evidence may include, but are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High impact BCS and their associated:	For those methods identified in Part 3.1	Examples of evidence may include, but

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	are not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events, per system capability: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use.
5.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify individuals who have authorized access to shared accounts.	Examples of evidence may include, but are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information:

None

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)	The Responsible Entity had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS. (Part 1.3)	The Responsible Entity neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity did not evaluate the cyber security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	The Responsible Entity did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR	The Responsible Entity did not include any processes for installing cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R2. (Requirement R2) OR The Responsible Entity did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	an existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)	OR The Responsible Entity did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)
R3	N/A	The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3). OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity missed one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	The Responsible Entity missed one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity missed two or more 15 calendar day intervals. (Part 4.4)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity, per system capability, did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity process(es) for password-only authentication for interactive user access did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity did not, per device capability, change known default passwords. (Part 5.4) OR The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity neither limited the number of unsuccessful authentication attempts nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-007-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses

Version	Date	Action	Change Tracking
			remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

Exhibit A-6

Proposed Reliability Standard CIP-007-7
Redline

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-~~6~~7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” ~~-~~For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1 Balancing Authority

    4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~4.1.6~~4.1.5 Reliability Coordinator

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~6~~7:

4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-~~5.1~~ identification and categorization processes.

~~5. Effective Dates:~~

~~See Implementation Plan for CIP-007-6.~~

~~6. Background:~~

~~Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *“Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].”* The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~” Columns in Tables:~~

~~5.1.~~4.3. ”: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies.~~ The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

5. ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~**Effective Dates:** See Project 2016-02 Modifications to CIP Standards Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R1 – ~~Ports and Services~~System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R1 – ~~Ports and Services~~System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control~~Medium Impact BES Cyber~~ Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA	~~Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.~~Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports ~~on all applicable Cyber Assets and Electronic Access Points, individually~~ or ~~by group.~~network accessible logical services, individually or by group; • Listings of the listening ports ~~on the Cyber Assets~~, individually or by group, from either ~~the device~~ configuration files or settings, command output (such as netstat), or network scans of open ports; ~~or~~

CIP-007-~~6~~7 Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part.		• Configuration ~~files~~or settings of host-based firewalls or other device level mechanisms that ~~only allow~~disable or prevent unneeded network accessible logical ports or network accessible logical services; or • Identity or process based access policy or workload configuration demonstrating needed ~~ports and deny all others.~~ network accessibility.

CIP-007-~~6~~7 Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting either: High impact BCS or their associated PCA. Medium impact BCS or their associated PCA.	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	A patch management process for tracking, evaluating, and installing cyber security patches~~ for applicable Cyber Assets~~. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for ~~applicable Cyber Assets~~Applicable Systems that are updateable and for which a patching source exists.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored~~, whether on an individual BES Cyber System or Cyber Asset basis. ~~.
2.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated:	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security~~-related~~ patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.		
2.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; ~~or~~ - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: - Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of ~~BES Cyber System Component~~component software revision, or registry exports that show software has been installed); or - A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.
2.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Manager or delegate.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R3 – Malicious Code Prevention

Part	Applicable Systems	Requirements	Measures
3.1	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Deploy method(s) to deter, detect, or prevent malicious code.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-~~6~~7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
	BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.		
3.3	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R4 – Security Event Monitoring

Part	Applicable Systems	Requirements	Measures
4.1	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Log security events ~~at the BES Cyber System level (~~, per ~~BES Cyber System~~system capability~~) or at the Cyber Asset level (per Cyber Asset capability)~~, for identification of, and after-the-fact investigations of, Cyber Security Incidents that ~~includes, as~~include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the ~~BES Cyber~~Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable~~	Generate alerts for security events that the Responsible Entity determines necessitates an alert~~,~~ that includes, as a minimum, each of the following types of events ~~(~~, per ~~Cyber Asset or BES Cyber System~~system capability~~):~~: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~6~~7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	logging.	
4.3	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	~~Where technically feasible, retain~~Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High ~~I~~impact ~~BES Cyber Systems~~ BCSand their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, ~~any~~ findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.1	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Have a method(s) to enforce authentication of interactive user access, ~~where technically feasible~~per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~6~~7 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use ~~for the BES Cyber System~~.
5.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify individuals who have authorized access to shared accounts.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~6~~7 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: - Records of a procedure that passwords are changed when new devices are in production; or - Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems~~Cyber Asset~~; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable Systems~~Cyber Asset~~.	Examples of evidence may include, but are not limited to: - System-generated reports or screenshots of the system-enforced password parameters, including length and complexity; or - Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~7 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.6	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	~~Where technically feasible, f~~For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	~~Where technically feasible, either:~~ Limit the number of unsuccessful authentication attempts~~;~~ or ~~G~~generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information:

None

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	~~R1~~The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)	The Responsible Entity~~ has implemented and documented processes for Ports and Services but~~ had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity ~~has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,~~ had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS. (Part 1.3)	The Responsible Entity ~~did not implement or document~~neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security~~	The Responsible Entity~~ has documented or implemented one or more process(es) for patch management but~~ did not include any processes,	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~7 Table R2. (Requirement R2) OR

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~patches for applicability but~~ did not evaluate the cyber security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	including the identification of sources, for tracking or evaluating cyber security patches for ~~applicable Cyber Assets. (~~Applicable Systems. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable	installing cyber security patches for ~~applicable Cyber Assets. (~~Applicable Systems. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but~~ did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch but~~ did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	evaluation completion. (Part 2.3)	
R3	N/A	The Responsible Entity ~~has implemented one or more documented process(es), but~~, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention, but~~, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3). OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity ~~has documented and~~	The Responsible Entity ~~has documented and~~	The Responsible Entity ~~has documented and~~	The Responsible Entity did not implement or document one or more process(es) that included

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~implemented~~ missed one ~~or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling~~ of ~~logged events at least every~~ 15 calendar ~~days but missed an~~day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	~~implemented~~ missed one ~~or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every~~ 15 calendar ~~days but missed an~~day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	~~implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but~~ did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity ~~has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but~~ did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity ~~has documented and implemented one or more process(es) to identify~~	the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity ~~has documented and implemented one or more process(es) to log events for the Applicable Systems (~~, per ~~device or~~ system capability~~)~~ ~~but~~, did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but~~ missed two or more 15 calendar day intervals. (Part 4.4)	
R5	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented~~ process(es) for password-only authentication for interactive user access ~~that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for~~	~~where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but~~ did not, per device capability, change known default passwords. (Part 5.4) OR ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the~~The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for~~

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	~~password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit~~neither limited the number of unsuccessful authentication attempts ~~or generate~~nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-007-7 Technical Rationale

~~None.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order

Version	Date	Action	Change Tracking
			No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.~~

~~**1.1.** This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'~~

~~**1.2.** Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.~~

~~The protection of these ports can be accomplished in several ways including, but not limited to:~~

~~Disabling all unneeded physical ports within the Cyber Asset's configuration~~

~~Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization~~

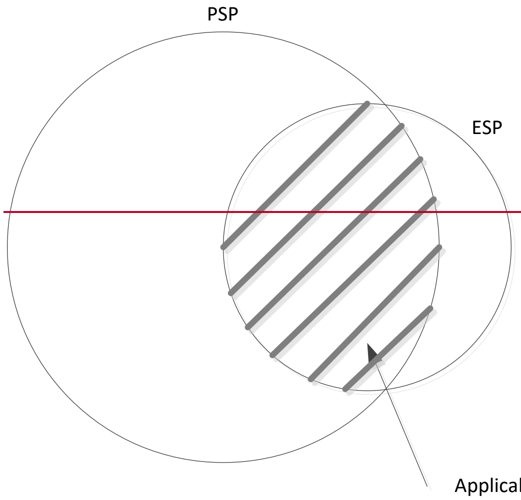
~~Physical port obstruction through removable locks~~

~~The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.~~

~~This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.~~

~~The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:~~

Location of Nonprogrammable Communication Components



Applicability of CIP-007-6 R1, Part 1.2 for Nonprogrammable Communication Components

~~**Requirement R2:**~~

~~The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.~~

~~Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.~~

~~One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.~~

~~**2.1.** The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they~~

~~can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.~~

~~**2.2.** Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.~~

~~When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.~~

~~**2.3.** The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or~~

~~those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.~~

~~**2.4.** The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.~~

~~**Requirement R3:**~~

~~**3.1.** Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.~~

~~**3.2.** When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or~~

~~method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.~~

~~Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.~~

~~**3.3.** In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.~~

~~**Requirement R4:**~~

~~Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.~~

~~**4.1.** In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.~~

~~Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.~~

~~User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.~~

~~It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.~~

~~**4.2.** Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.~~

~~The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:~~

~~Detected known or potential malware or malicious activity~~

~~Failure of security event logging mechanisms~~

~~Login failures for critical accounts~~

~~Interactive login of system accounts~~

~~Enabling of accounts~~

~~Newly provisioned accounts~~

~~System administration or change tasks by an unauthorized user~~

~~Authentication attempts on certain accounts during non-business hours~~

~~Unauthorized configuration changes~~

~~Insertion of Removable Media in violation of a policy~~

~~**4.3** Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.~~

~~**4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-~~

~~time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.~~

~~Requirement R5:~~

~~Account types referenced in this guidance typically include:~~

~~Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.~~

~~Individual user account: An account used by a single user.~~

~~Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.~~

~~System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.~~

~~Application account: A specific system account, with rights granted at the application level often used for access into a Database.~~

~~Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.~~

~~Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.~~

~~Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.~~

~~5.1~~ ~~Reference the Requirement's rationale.~~

~~5.2~~ ~~Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.~~

~~5.3~~ ~~Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.~~

~~5.4.~~ ~~Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.~~

~~The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or~~

~~installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.~~

~~**5.5.** Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.~~

~~Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.~~

~~**5.6** Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.~~

~~**5.7** Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.~~

~~Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.~~

~~In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.~~

~~The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).~~

~~Rationale for Requirement R2:~~

~~Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.~~

~~Rationale for Requirement R3:~~

~~Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.~~

~~Rationale for Requirement R4:~~

~~Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.~~

~~Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.~~

~~**Rationale for Requirement R5:**~~

~~To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.~~

~~Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.~~

~~Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.~~

~~Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.~~

~~For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.~~

~~The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.~~

~~The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.~~

~~The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.~~

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-7

Proposed Reliability Standard CIP-008-7
Clean

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the Bulk Electric System (BES):

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

   4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BES) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated Electronic Access Control and Monitoring Systems (EACMS) Medium impact BCS and their associated EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the Applicable Systems column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column including justification for attempt determination criteria and documented processes for notification.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the Applicable Systems column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	Examples of evidence may include, but are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the	Examples of evidence may include, but are not limited to: 1. Dated and revised Cyber Security Incident response plan with changes

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column according to the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and CISA, or their successors.
4.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the Applicable Systems column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and CISA, or their successors.

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and CISA, or their successors.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible Entity's plan did not include one or more processes to provide notification per Requirement R4. (Part 1.2) OR The Responsible Entity's plan did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	The Responsible Entity did not develop a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible Entity's plan did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the Applicable Systems column for Part 1.2. (Part 1.2)
R2	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Par 2.1)	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Part 2.1) OR	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not retain relevant records related

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column for Part 2.2 occurs. (Part 2.2)	to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the Applicable Systems column for Part 2.3. (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR The Responsible Entity did not update the Cyber Security	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1) OR The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-008-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td>Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan:
• Roles or responsibilities, or
• Cyber Security Incident response groups or individuals, or
• Technology changes. (Part 3.2)</td><td>calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan:
• Roles or responsibilities, or
• Cyber Security Incident response groups or individuals, or
• Technology changes. (Part 3.2)</td><td></td></tr>
<tr><td>R4</td><td>The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2)
OR
The Responsible Entity did not report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3)
OR
The Responsible Entity did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)</td><td>The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column. (Requirement R4)</td><td>The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2)
OR
The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)</td><td>The Responsible Entity did not notify E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)</td></tr>
</table>

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-008-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Version	Date	Action	Change Tracking
7	TBD	Virtualization Modifications	

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-7

Proposed Reliability Standard CIP-008-7
Redline

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-~~6~~7

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the ~~BES:~~Bulk Electric System (BES):

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Remedial Action Scheme~~RAS where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-~~6~~7:

4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BES) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. ~~5. Effective Dates:~~

~~See Implementation Plan for CIP-008-6.~~

~~6. Background:~~

~~Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~” Columns in Tables:~~
”: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies.~~ The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~6~~7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~6~~7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-~~6~~7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated~~:~~ Electronic Access Control and Monitoring Systems (EACMS) Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the “Applicable Systems” column	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column including justification for attempt determination criteria and documented processes for notification.

CIP-008-~~6~~7 Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
		for this Part; and 1.2.3 To provide notification per Requirement R4.	
1.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-~~6~~7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-~~6~~7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-~~6~~7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every~~-~~ 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-~~6~~7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the ~~"~~"Applicable Systems~~"~~" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the ~~"~~"Applicable Systems~~"~~" column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-~~6~~7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-~~6~~7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-~~6~~7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, all of the following: 1. Dated documentation of~~-~~ post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or ~~•~~ Training sign-in sheets. •

~~CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication~~			
~~**Part**~~	~~**Applicable Systems**~~	~~**Requirements**~~	~~**Measures**~~
3.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the	~~An example~~Examples of evidence may include, but ~~is~~are not limited to: 1. Dated and revised Cyber Security Incident response plan with changes

CIP-008-~~6~~7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
	Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States ~~National~~ Cybersecurity ~~and Communications Integration Center (NCCIC),~~~~[1]~~& Infrastructure Security Agency (CISA), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the ~~"~~Applicable Systems~~"~~ column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-~~6~~7 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column according to the applicable requirement parts in *CIP-008-~~6~~7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-~~6~~7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and ~~4.1.3~~ The level of intrusion that was achieved or attempted. 4.1.3	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and ~~NCCIC.~~ CISA, or their successors.
4.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines:	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ~~NCCIC.~~ CISA, or their successors.

~~[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).~~

CIP-008-~~6~~7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	- One hour after the determination of a Reportable Cyber Security Incident. By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column for this Part. -	
4.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within ~~7~~seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and ~~NCCIC.~~CISA, or their successors.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~
- ~~Complaint~~

~~**1.4. Additional Compliance Information:**~~

~~None~~

~~2. Table of Compliance Elements~~

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-008-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible ~~Entity has developed a Cyber Security Incident response plan, but the plan does~~Entity's plan did not include one or more processes to provide notification per Requirement R4. (Part 1.2) OR The Responsible ~~Entity has developed a Cyber Security Incident response plan, but~~	The Responsible Entity ~~has~~did not ~~developed~~develop a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible ~~Entity has developed a Cyber Security Incident response~~Entity's plan~~, but the plan does~~ did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the ~~“~~Applicable Systems~~”~~ column for Part 1.2. (Part 1.2)

R #	Violation Severity Levels (CIP-008-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~the plan does~~Entity’s plan did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	
R2	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Par 2.1)	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column for Part 2.2 occurs. (Part 2.2)	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column for Part 2.3. (Part 2.3)
R3	The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120	The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response	The Responsible Entity~~ has~~ neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a	The Responsible Entity~~ has~~ neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response

R #	Violation Severity Levels (CIP-008-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or	Reportable Cyber Security Incident. (Part 3.1.1) OR The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	to a Reportable Cyber Security Incident. (Part 3.1.1)

R #	Violation Severity Levels (CIP-008-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		• Technology changes. (Part 3.2)		
R4	The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to~~did not notify or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR ~~The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to~~The Responsible Entity did not report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3)	The Responsible Entity ~~failed to~~did not notify E-ISAC or ~~NCCIC~~CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the ~~"~~Applicable Systems~~"~~ column. (Requirement R4)	The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to~~did not notify or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity ~~failed to~~did not notify E-ISAC or ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	The Responsible Entity ~~failed to~~did not notify E-ISAC and ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Violation Severity Levels (CIP-008-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to~~did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-008-7 Technical Rationale

~~None.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

7	TBD	Virtualization Modifications	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-8

Proposed Reliability Standard CIP-009-7
Clean

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

   4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	Examples of evidence may include, but are not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover Applicable System functionality.
1.4	High impact BCS and their associated:	One or more processes to verify the	Examples of evidence may include, but are

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and PACS	successful completion of the backup processes in Part 1.3 and to address any backup failures.	not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Examples of evidence may include, but are not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: - By recovering from an actual incident; - With a paper drill or tabletop exercise; or - With an operational exercise.	Examples of evidence may include, but are not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover Applicable System functionality substitutes for this test.	Examples of evidence may include, but are not limited to, operational logs or test results with criteria for testing the usability (e.g., sample tape load, browsing tape contents) and compatibility with current system configurations (e.g., manual, or automated comparison checkpoints between backup media contents and current configuration).
2.3	High impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.	Examples of evidence may include, but are not limited to, dated documentation of: - An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
		An actual recovery response may substitute for an operational exercise.	• An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable Requirement Parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the Applicable Requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a	Examples of evidence may include, but are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to:

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
		defined role in the recovery plan of the updates.	• Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:
As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:
The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information: None

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity's plan(s) did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity plan(s) did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity did not create recovery plan(s) for Applicable Systems. OR The Responsible Entity plan(s) did not address the conditions for activation in Part 1.1. OR The Responsible Entity plan(s) did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 15 calendar months, not exceeding 16	The Responsible Entity did not test the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Part 2.2)	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 17 calendar months, not exceeding 18	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 18 calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan(s)

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-009-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>calendar months between tests. (Part 2.2)
OR
The Responsible Entity did not test the recovery plan according to Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)</td><td>OR
The Responsible Entity did not test the recovery plan according to Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)</td><td>calendar months between tests. (Part 2.2)
OR
The Responsible Entity did not test the recovery plan according to Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)</td><td>according to Part 2.3 within 39 calendar months between tests of the plan(s). (Part 2.3)</td></tr>
<tr><td>R3</td><td>The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Part 3.1.3)</td><td>The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2)
OR
The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3)
OR
The Responsible Entity did not update the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days</td><td>The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1)
OR
The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2)
OR
The Responsible Entity did not update the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the</td><td>The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1)</td></tr>
</table>

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
		of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part 3.2)	following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-009-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-8

Proposed Reliability Standard CIP-009-7
Redline

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-~~6~~7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES~~.~~).

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 **Balancing Authority**

4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 **Generator Operator**

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~**4.1.6**~~**4.1.5 Reliability Coordinator**

~~**4.1.7**~~**4.1.6 Transmission Operator**

~~**4.1.8**~~**4.1.7 Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 ~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme~~Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-~~6~~7:

4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3**~~**4.2.3.4** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4**~~**4.2.3.5** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.5**~~**4.2.3.6** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

~~**5. Effective Dates:**~~

~~See Implementation Plan for CIP-009-6.~~

~~**6. Background:**~~

~~Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident~~

~~response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~” Columns in Tables:~~

~~5.1.~~4.3. ”: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies. ~~The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

- ~~**Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems at Control Centers –** Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS) –** Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.~~

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

- ~~**Physical Access Control Systems (PACS) –** Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*.

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7 Table R1 – Recovery Plan Specifications*.

CIP-009-~~6~~7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-~~6~~7 Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover ~~BES Cyber~~Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover ~~BES Cyber~~Applicable System functionality.
1.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; and PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Examples ~~An example~~ of evidence may include, but are not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High i~~I~~mpact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium i~~I~~mpact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per system ~~Cyber Asset~~ capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Examples ~~An example~~ of evidence may include, but are not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-~~6~~7 Table R2 – Recovery Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: - By recovering from an actual incident; - With a paper drill or tabletop exercise; or - With an operational exercise.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
2.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and	Test a representative sample of information used to recover ~~BES Cyber~~Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover ~~BES Cyber~~Applicable System functionality substitutes for this test.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, operational logs or test results with criteria for testing the usability (e.g.~~.~~, sample tape load, browsing tape contents) and compatibility with current system configurations (e.g.~~.~~, manual, or automated comparison checkpoints between backup media contents and current configuration).

CIP-009-~~6~~7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~2.~~ PACS ~~3.~~2.		
2.3	High ~~Impact BES Cyber Systems~~impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the ~~applicable requirement~~Applicable Requirement parts in *CIP-009-~~6~~7 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-~~6~~7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact ~~-~~the ability to execute the recovery plan:	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or

CIP-009-~~6~~7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information: None

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible ~~Entity has developed recovery~~Entity's plan(s~~), but the plan(s) do~~) did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity ~~has developed recovery~~ plan(s~~), but the plan(s) do~~) did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity ~~has~~did not ~~created~~create recovery plan(s) for ~~BES Cyber~~Applicable Systems. OR The Responsible Entity ~~has created recovery~~ plan(s) ~~for BES Cyber Systems, but the plan(s) does~~did not address the conditions for activation in Part 1.1. OR The Responsible Entity ~~has created recovery plan(s) for BES Cyber Systems, but the plan(s) does~~plan(s) did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.1 within 15 calendar months, not exceeding 16 calendar months between	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1) OR	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Part 2.1)	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR

R #	Violation Severity Levels (CIP-009-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	tests of the plan~~. (~~(s). (Part 2.1) OR The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan according to ~~R2~~ Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)	The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan according to ~~R2~~ Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)	OR The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan according to ~~R2~~ Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)	The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 18 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.3 within 39 calendar months between tests of the plan~~. (~~(s). (Part 2.3)
R3	The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar	The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan

R #	Violation Severity Levels (CIP-009-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	days of the update being completed. (Part 3.1.3)	plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3) OR The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or ~~–~~responsibilities, or • Responders, or • Technology changes. (Part 3.2)	recovery plan test or actual recovery. (Part 3.1.1) OR The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	test or actual recovery. (Part 3.1.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-009-7 Technical Rationale

~~None.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~The following guidelines are available to assist in addressing the required components of a recovery plan:~~

- ~~NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf~~
- ~~National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf~~

~~The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.~~

~~A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.~~

~~For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.~~

~~For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.~~

~~For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:~~

1. ~~Installation files and media;~~
2. ~~Current backup tapes and any additional documented configuration settings;~~
3. ~~Documented build or restoration procedures; and~~
4. ~~Cross site replication storage.~~

~~For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:~~

- ~~Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.~~
- ~~Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.~~
- ~~Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.~~
- ~~Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.~~

~~The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.~~

~~For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.~~

~~Requirement R2:~~

~~A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.~~

~~A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.~~

~~Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."~~

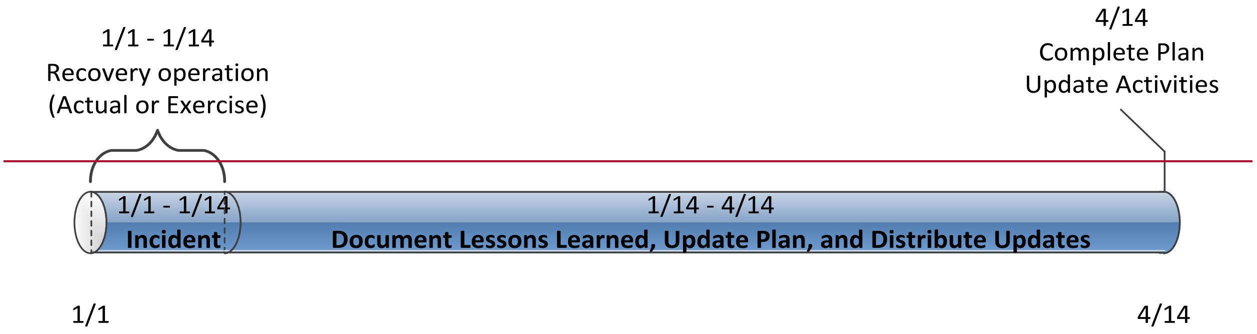
~~The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."~~

~~For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.~~

~~**Requirement R3:**~~

~~This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.~~

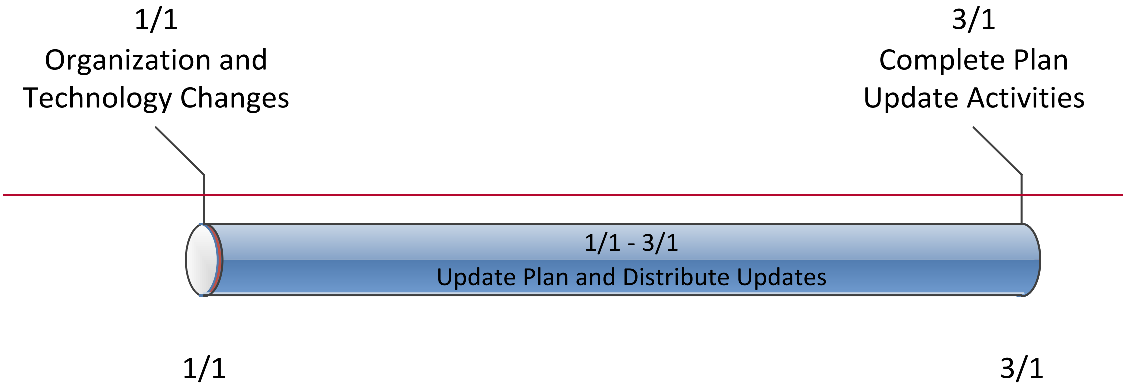
~~The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.~~



~~**Figure 1: CIP-009-6 R3 Timeline**~~

~~The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.~~

~~The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.~~



~~**Figure 2: Timeline for Plan Changes in 3.2**~~

~~When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.~~

~~Rationale for Requirement R2:~~

~~The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.~~

~~Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.~~

~~Rationale for Requirement R3:~~

~~To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.~~

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-9

Proposed Reliability Standard CIP-010-5
Clean

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and

data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.	Examples of evidence may include, but are not limited to, one or more documented process(es) that authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity, such as: • Change records documenting the authorization. • Change records authorizing systems to automate changes to Applicable Systems. Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) • Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) • Configuration of malicious code prevention methods (CIP-007 R3) • Configuration of security event logging/alerting (CIP-007 R4) • Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5) • Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)
1.2	High impact BCS	1.2.1. Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, to ensure that required cyber security controls in CIP-005 and CIP-007 are not	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test, or logs from systems that automatically remediate deviations in required cyber security controls in CIP-005 and CIP-007.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		adversely affected; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.
1.4	High impact BCS and their associated: 1. EACMS;	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the altered cyber security controls were not	An example of evidence may include, but is not limited to:

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	adversely affected.	• System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods;	An example of evidence may include, but is not limited to, documented methods to monitor at least once every 35 calendar days. Monitoring system configuration or procedural controls demonstrating monitoring of at least one cyber security control for 2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	Applicable Systems	Requirements	Measures
		2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements or additions with a previously assessed configuration of an existing Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of tools used to perform the assessment; or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of evidence may include, but are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA, and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.		The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity change management process(es) did not include authorization for changes as required in Part 1.1. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. (Part 1.2); OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) OR The Responsible Entity's change management process(es) does not include verification, as required by Part 1.4. (Part 1.4)	The Responsible Entity neither documented nor implemented any change management process(es) that include required items in Part 1.1 through Part 1.4. (Requirement R1)
R2.	The Responsible Entity did not monitor within 35 calendar days, but less than 70 calendar days as required by Part 2.1.	The Responsible Entity's documented and implemented configuration monitoring process(es) does not include one or two of the required	The Responsible Entity's documented and implemented configuration monitoring process(es) does not include three or four of the required	The Responsible Entity neither documented nor implemented a configuration monitoring process(es); or the process does not include five or more

R #	**Violation Severity Levels**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
		Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 70 calendar days, but less than 105 calendar days as required by Part 2.1.	Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 105 calendar days, but less than 140 calendar days as required by Part 2.1.	of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 140 calendar days or more as required by Part 2.1. OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1)
R3.	The Responsible Entity performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity did not implement any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3) OR The Responsible Entity performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2) OR The Responsible Entity did not perform the active vulnerability assessment of a Cyber System prior to it becoming an Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)
R4.	The Responsible Entity did not manage its Transient Cyber Asset(s) according to Attachment 1, Section 1.1. (Requirement R4)	The Responsible Entity did not implement the Removable Media sections according to Attachment 1, Section 3. (Requirement R4)	The Responsible Entity did not authorize its TCA(s) according to Attachment 1, Section 1.2. (R4)	The Responsible Entity did not document or implement one or more plan(s) for TCAs and Removable Media according to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity did not document the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document authorization for TCA managed by the Responsible Entity according to Attachment 1, Section 1.2. (Requirement R4)	OR The Responsible Entity did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCA managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	OR The Responsible Entity did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	Requirement R4. (Requirement R4)

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-010-5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	
4	3/18/2021	FERC order approving Docket No. RD21-2-000	
4	4/5/2021	Effective Date	10/1/2022
5	TBD	Virtualization Modifications	

Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Live operating system and software executable only from read only media;
- System hardening; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read only media;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

2.3. For any method used as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCA(s). This can be included as part of the TCA(s), part of the documentation related to authorization of TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating system and software executable only from read only media, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the risk of software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, methods to maintain the known good state of the OS and all software, or system hardening practices. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail,

policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that that document a review of the use of live operating system and software executable only from read only media; memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that that document a review of the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, and system hardening by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-9

Proposed Reliability Standard CIP-010-5
Redline

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

~~1.~~2. Number: CIP-010-~~4~~5

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting ~~BES Cyber Systems~~BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

~~2.~~4. Applicability:

~~2.1.~~4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

~~2.2.~~4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-~~4~~5:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.5.**~~**4.2.3.6.** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

~~**3. Effective Date:** See Implementation Plan for Project 2019-03.~~

~~**4. Background:** Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the~~

~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

"Applicable Systems~~" Columns in Tables:~~

4.3. ": Each table has an "Applicable Systems" column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies.~~ The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~

- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-45 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-45 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-45 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
~~**1.1**~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2.1. PACS; and~~ ~~3.1. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Develop a baseline configuration, individually or by group, which shall include the following items:~~ ~~1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;~~ ~~1.1.2. Any commercially available or open-source application software (including version) intentionally installed;~~ ~~1.1.3. Any custom software installed;~~ ~~1.1.4. Any logical network accessible ports; and~~ ~~1.1.5. Any security patches applied.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or~~ ~~• A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.~~
~~**1.2**~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~	~~Authorize and document changes that deviate from the existing baseline configuration.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• A change request record and~~

CIP-010-45 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~		~~associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or~~ ~~• Documentation that the change was performed in accordance with the requirement.~~
~~1.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.~~	~~An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.~~
1.41	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); ~~1.~~ Physical Access Control~~EACMS;~~ ~~2.~~1. ~~PACS; and~~ ~~3.~~1. ~~PCA~~ 2. ~~Medium Impact BES Cyber~~ Systems (PACS); and	~~For a change~~Authorize changes that ~~deviates from~~affect Applicable Systems where those changes alter the ~~existing baseline configuration:~~ ~~1.4.1. Prior to the change, determine required~~behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 ~~and~~or CIP-007 ~~that~~	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, ~~a list~~one or more documented process(es) that authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls ~~verified or tested along with the dated test results.~~, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity, such as:

CIP-010-~~4~~5 Table R1 – ~~-~~Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
	3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: ~~4.~~1. EACMS; ~~5.~~2. PACS; and ~~6.~~3. PCA SCI supporting an Applicable System in this Part.	~~could be impacted~~, as defined by the ~~change;~~ ~~1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and~~ ~~Document the results of the verification~~Responsible Entity.	• Change records documenting the authorization. • Change records authorizing systems to automate changes to Applicable Systems. Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) • Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) • Configuration of malicious code prevention methods (CIP-007 R3) • Configuration of security event logging/alerting (CIP-007 R4) • Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5)

CIP-010-~~4~~5 Table R1 – ~~-~~Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			- Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)
1.~~5~~2	High ~~Impact BES Cyber Systems~~impact BCS	~~Where technically feasible, for each change that deviates from the existing baseline configuration:~~ 1.2.1. Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, ~~that models the baseline configuration~~ to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test~~.~~ , or logs from systems that automatically remediate deviations in required cyber security controls in CIP-005 and CIP-007.
1.~~6~~3	High ~~Impact BES Cyber Systems~~impact	Prior to ~~a change that deviates from~~ the	An example of evidence may include, but is

CIP-010-~~4~~5 Table R1 – ~~-~~Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	~~existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5,~~installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.~~6~~3.1.~~–~~ Verify the identity of the software source; and 1.~~6~~3.2.~~–~~ Verify the integrity of the software obtained from the software source.	not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to ~~the baseline change~~installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.
1.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the altered cyber security controls were not adversely affected.	An example of evidence may include, but is not limited to: • System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

CIP-010-45 Table R1 – -Configuration Change Management

Part	Applicable Systems	Requirements	Measures

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-~~4~~5 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~4~~5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~4~~5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact~~impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	~~Monitor~~Methods to monitor, per system capability, at least once every 35 calendar days, for ~~changes to~~ unauthorized changes that affect Applicable Systems, where those changes alter the ~~baseline configuration (as described~~behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in ~~Requirement R1, Part~~ CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1~~).~~. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.	An example of evidence may include, but is not limited to, ~~logs from a~~documented methods to monitor at least once every 35 calendar days. Monitoring system ~~that is monitoring the~~ configuration or procedural controls demonstrating monitoring of at least one cyber security control for 2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

CIP-010-45 Table R2 – -Configuration Monitoring

Part	Applicable Systems	Requirements	Measures
		2.1.4. Configuration of malicious code protection methods; 2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~3~~5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~4~~5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~Impact~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every -15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~4~~5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~Impact~~impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	~~Where technically feasible, at~~At least once every 36 calendar months, per system capability: ~~2.2.1~~3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects~~, that models the baseline configuration of the BES Cyber System in a production environment~~; and ~~2.2.2~~3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-45 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Prior to ~~adding~~becoming a new ~~applicable Cyber Asset to a production environment~~Applicable System, perform an active vulnerability assessment of the new ~~Cyber Asset~~Applicable System, except for ~~CIP Exceptional Circumstances and like~~: • Like replacements ~~of the same type of Cyber Asset~~or additions with a ~~baseline~~previously assessed configuration ~~that models~~of an existing ~~baseline configuration of the previous or other existing Cyber Asset.~~Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to~~, a document listing~~: • The output of tools used to perform the assessment; or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment ~~(~~performed prior to ~~the commissioning of the~~ becoming a new ~~Cyber Asset) and the output of any tools used to perform the assessment.~~ Applicable System.

CIP-010-~~4~~5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to~~, a document~~: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA, and associated ~~Protected Cyber Assets~~SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for ~~Transient Cyber Assets~~TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for ~~Transient Cyber Assets~~TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use ~~Transient Cyber Asset~~TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use ~~Transient Cyber Asset~~TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)~~	The Responsible ~~Entity has documented and implemented a configuration~~Entity's change management process(es) ~~that includes only three~~does not include one of the required ~~baseline~~ items listed in 1.~~1~~2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.~~5. (~~3.1~~.~~ through 1.3.2. (Part 1.3)	The Responsible Entity ~~has documented and implemented a configuration~~ change management process(es) ~~that includes only two of the~~ did not include authorization for changes as required ~~baseline~~in Part 1.1. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.~~1~~2.1 through 1.2.2. (Part 1.~~5. (1.1)~~2); OR The Responsible ~~Entity has a~~Entity's change management process ~~as specified in Part 1.6 to verify the identity of the software source (1.6.1) but~~(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) OR ~~have a~~The Responsible Entity's change management process ~~as specified in~~ (es)	The Responsible Entity ~~has not~~neither documented ~~or~~nor implemented any ~~configuration change management process(es). (R1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration~~ change management process(es) that ~~includes only one of the~~include required ~~baseline~~ items ~~listed~~ in Part 1.~~1.~~1 through ~~1.1.5. (1.1)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2~~Part ~~)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) to~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			does not include verification, as required by Part 1.~~6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2~~4. (Part 1.4)	~~update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (~~1.4.~~1~~ (Requirement R1) ~~OR~~ ~~The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~following the change. (1.4.2 & 1.4.3)~~ ~~OR~~ ~~The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1)~~ ~~OR~~ ~~The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)~~ ~~OR~~ ~~The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)~~
R2.	~~N/A~~The Responsible Entity did not monitor within 35 calendar days, but less than 70 calendar days as required by Part 2.1.	~~N/A~~The Responsible Entity's documented and implemented configuration monitoring process(es) does not include one or two of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 70 calendar days, but less than 105 calendar days as required by Part 2.1.	~~N/A~~The Responsible Entity's documented and implemented configuration monitoring process(es) does not include three or four of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 105 calendar days, but less than 140 calendar days as required by Part 2.1.	The Responsible Entity ~~has not~~neither documented ~~or~~nor implemented a configuration monitoring process(es~~) to~~); or the process does not include five or more of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor ~~for, investigate, and document~~within 140 calendar days or more as required by Part 2.1. OR The Responsible Entity neither documented nor investigated detected unauthorized changes ~~to the baseline at least once every 35 calendar days. (~~. (Part 2.1)
R3.	The Responsible Entity ~~has implemented one or more documented vulnerability~~	The Responsible Entity ~~has implemented one or more documented vulnerability~~	The Responsible Entity ~~has implemented one or more documented vulnerability~~	The Responsible Entity ~~has~~did not ~~implemented~~implement any vulnerability assessment

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.1) OR The Responsible Entity~~ has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.2)	~~assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.1) OR The Responsible Entity~~ has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.2)	~~assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.1) OR The Responsible Entity~~ has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.2)	processes for one of its ~~applicable BES Cyber~~Applicable Systems. (Requirement R3) OR The Responsible Entity~~ has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity~~ has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems~~.(~~. (Part 3.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity ~~has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but~~ did not perform the active vulnerability assessment ~~in~~of a ~~manner that models~~Cyber System prior to it becoming an ~~existing baseline configuration of its applicable BES Cyber~~Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its ~~applicable BES Cyber~~Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				plan, and the execution status of the mitigation plans. (Part 3.4)
R4.	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not manage its Transient Cyber Asset(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.1. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document the Removable Media sections according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document authorization for ~~Transient~~	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement the Removable Media sections according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to~~did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not authorize its ~~Transient Cyber Asset~~TCA(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCAs managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR	The Responsible Entity ~~failed to~~did not document or implement one or more plan(s) for ~~Transient Cyber Assets~~TCAs and Removable Media according to ~~CIP-010-4,~~ Requirement R4. (Requirement R4)

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	~~Cyber Assets~~TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (Requirement R4)	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for ~~Transient Cyber Assets~~TCAs managed by a party other than the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan~~ for Project 2019-03.~~”.
- CIP-010-45 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. -Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	
4	3/18/2021	FERC order approving Docket No. RD21-2-000	
4	4/5/2021	Effective Date	10/1/2022
5	TBD	Virtualization Modifications	

Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. ~~Transient Cyber Asset~~TCA(s) Managed by the Responsible Entity.

1.1. ~~Transient Cyber Asset~~TCA Management: Responsible Entities shall manage ~~Transient Cyber Asset~~TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection ~~to a BES Cyber System~~, or (3) a combination of both (1) and (2) above.

1.2. ~~Transient Cyber Asset~~TCA Authorization: For each individual or group of ~~Transient Cyber Asset~~TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset (per Transient Cyber Asset~~TCA (per TCA capability):

- Security patching, including manual or managed updates;
- ~~Live operating system and software executable only from read-only media;~~
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; ~~or~~
- Live operating system and software executable only from read only media;
- System hardening; or

- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of ~~Transient Cyber Asset~~TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. ~~Transient Cyber Asset~~TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset (per Transient Cyber Asset~~TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- ~~Other~~Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read~~-~~ only media;
- Review of system hardening used by the party; or
- ~~Other~~Review of other method(s) to mitigate the risk of introduction of malicious code.

2.3. For any method used ~~to mitigate software vulnerabilities or malicious code~~ as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset~~TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code ~~to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets~~, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media ~~using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets~~prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code ~~on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets~~.

CIP-010-~~4~~5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the ~~Transient Cyber Asset~~TCA(s). This can be included as part of the ~~Transient Cyber Asset plan~~TCA(s), part of the documentation related to authorization of ~~Transient Cyber Asset~~TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of ~~Transient Cyber Asset~~TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating ~~systems~~ system and software executable only from read~~-~~only media, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the risk of software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, methods to maintain the known good state of the OS and all software, or ~~procedures or processes associated with~~ system hardening practices. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that that document a review of the use of live operating system and software executable only from read only media; memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that that document a review of the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, ~~use of live of operating systems or~~and system hardening ~~performed~~ by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Exhibit A-10

Proposed Reliability Standard CIP-011-4
Clean

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-4

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1 Balancing Authority

    4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3 Generator Operator

    4.1.4 Generator Owner

    4.1.5 Reliability Coordinator

    4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-4:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards” Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BCSI pertaining to Applicable Systems identified in *CIP-011-4 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include

CIP-011-4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part		topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-4 Table R2 –Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4 Table R2 –Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).	Examples of evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

B. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-011-4)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not implement one or more BCSI protection program(s). (Requirement R1) OR The Responsible Entity did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity did not include processes for reuse to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity did not include disposal processes to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity neither documented nor implemented any processes for applicable requirement parts in CIP-011-4 Table R2 –Reuse and Disposal. (Requirement R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-011-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
3	12/7/21	FERC Order issued approving CIP-011-3 Docket No. RD21-6-000	“A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability

Version	Date	Action	Change Tracking
			Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.”
3	12/10/21	Effective Date	1/1/2024
4	TBD	Virtualization Modifications	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-10

Proposed Reliability Standard CIP-011-4
Redline

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:**~~-~~ CIP-011-~~3~~4

3. **Purpose:**~~-~~ To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

~~3.~~4. **Applicability:**

~~3.1.~~4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

~~3.1.1~~4.1.1 **Balancing Authority**

~~3.1.2~~4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

~~3.1.2.1~~4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

~~3.1.2.1.1~~4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

~~3.1.2.1.2~~4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

~~3.1.2.2~~4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.1.2.3~~4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.1.2.4~~4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~3.1.3~~4.1.3 **Generator Operator**

~~3.1.4~~4.1.4 **Generator Owner**

~~3.1.5~~4.1.5 **Reliability Coordinator**

~~3.1.6~~4.1.6 **Transmission Operator**

~~3.1.7~~4.1.7 **Transmission Owner**

~~3.2.~~4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

~~3.2.1~~4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

~~3.2.1.1~~4.2.1.1 Each UFLS or UVLS System that:

~~3.2.1.1.1~~4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

~~3.2.1.1.2~~4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

~~3.2.1.2~~4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.2.1.3~~4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.2.1.4~~4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~3.2.2~~4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers:** All BES Facilities.

~~3.2.3~~4.2.3 **Exemptions:** The following are exempt from Standard CIP-011-~~3~~4:

~~3.2.3.1~~4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

~~3.2.3.2~~4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~3.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~3.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~3.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5.1a~~ identification and categorization processes.

~~**1. Effective Dates:** See Implementation Plan for CIP-011-3.~~

~~**2. Background:** Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and~~

~~implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~” Columns in Tables:~~

~~3.3.~~4.3. ”: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies. ~~The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards” Implementation Plan.

- B. ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

Requirements and Measures

R1. ~~**R1.**~~ Each Responsible Entity shall implement one or more documented information protection program(s) for ~~BES Cyber System Information (~~BCSI~~)~~ pertaining to ~~"~~Applicable Systems~~"~~ identified in *CIP-011-~~3~~4 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-~~3~~4 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1.~~-~~ Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~3~~4 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~3~~4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of ~~acceptable~~ evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High ~~I~~impact BCS and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following:

CIP-011-~~3~~4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part		- Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or - Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: - Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or - Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or - Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~3~~4 Table R2 –~~ BES Cyber Asset~~ Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2.~~-~~ Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~3~~4 Table R2 –~~ BES Cyber Asset~~ Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~3~~4 Table R2 –~~ BES Cyber Asset~~ Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Prior to the release for~~Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse ~~of applicable Cyber Assets that contain BCSI~~ (except for reuse within other systems identified in the ~~“~~"Applicable Systems~~”~~" column~~), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.~~).	Examples of~~ acceptable~~ evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

B. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-011-~~3~~4)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~documented, but~~ did not~~,~~ implement one or more BCSI protection program(s). ~~(~~ (Requirement R1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity ~~implemented one or more~~ ~~documented~~did not include processes for reuse to prevent the unauthorized retrieval of BCSI from ~~the BES Cyber Asset~~an Applicable System. (Part 2.1)	The Responsible Entity ~~implemented one or more~~ ~~documented~~did not include disposal processes to prevent the unauthorized retrieval of BCSI from an Applicable System~~the BES Cyber Asset~~. (Part 2.1)	The Responsible Entity ~~has not~~neither documented ~~or~~ nor implemented any processes for applicable requirement parts in CIP-011-4 Table R2 –Reuse and Disposal. (Requirement R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-011-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
3	12/7/21	FERC Order issued approving CIP-011-3 Docket No. RD21-6-000	“A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability

Version	Date	Action	Change Tracking
			Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.”
3	12/10/21	Effective Date	1/1/2024
4	TBD	Virtualization Modifications	

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-11

Proposed Reliability Standard CIP-013-3
Clean

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

        4.1.1. Balancing Authority

        4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

            4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

                4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

                4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

            4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

            4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

        4.1.3. Generator Operator

        4.1.4. Generator Owner

        4.1.5. Reliability Coordinator

        4.1.6. Transmission Operator

        4.1.7. Transmission Owner

    4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in

this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider:** One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers:** All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-013-3:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable systems listed in Requirement R1 to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring applicable systems listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's supply chain cyber risk management plan(s) did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1. OR The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in Requirement R1.
R2.	The Responsible Entity did not implement one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity did not implement the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1, and did not implement the use of process(es) for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				procuring applicable systems as specified in Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in Requirement R2.
R3.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 16th calendar month since the previous review.	The Responsible Entity exceeded the 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 17th calendar month since the previous review.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 18th calendar month since the previous review.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-013-3 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	
2	3/18/2021	FERC Order approving CIP-013-2. Docket No. RD21-2-000.	
2	4/5/2021	Effective Date	10/1/2022
3	TBD	Virtualization Modifications	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-11

Proposed Reliability Standard CIP-013-3
Redline

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-~~2~~3**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems~~.~~ (BCS).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in

this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider:** One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers:** All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-013-~~2~~3:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.5.**~~**4.2.3.6.** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan~~ for Project 2019-03.~~”.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact ~~BES Cyber Systems~~BCS and their associated Electronic Access Control or Monitoring Systems (EACMS~~) and~~), Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of ~~BES Cyber Systems and their associated EACMS and PACS~~applicable systems listed in Requirement R1 to identify and assess cyber security risk(s) to the ~~Bulk Electric System~~BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring ~~BES Cyber Systems, and their associated EACMS and PACS,~~applicable systems listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor~~ for use in the BES Cyber System and their associated EACMS and PACS~~; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible ~~Entity developed one or more documented~~Entity's supply chain cyber ~~security~~ risk management plan(s) ~~which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do~~did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible ~~Entity developed one or more documented~~Entity's supply chain cyber security risk management plan(s) ~~which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do~~did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible ~~Entity developed one or more documented~~Entity's supply chain cyber security risk management plan(s~~), but the plan(s~~) did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~applicable systems as specified in Part 1.1~~, or the~~. OR The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~applicable systems as specified in Part 1.2.	The Responsible ~~Entity developed one or more documented~~Entity's supply chain cyber security risk management plan(s~~), but the plan(s~~) did not include the use of process(es) in planning for procurement ~~of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~applicable systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				cyber security risk management plan(s) as specified in ~~the~~ Requirement R1.
R2.	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but~~ did not implement one of the parts in ~~Requirement R1~~ Part 1.2.1 through Part 1.2.6.	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but~~ did not implement two or more of the parts in ~~Requirement R1~~ Part 1.2.1 through Part 1.2.6.	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or~~ did not implement the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~applicable systems as specified in ~~Requirement R1~~ Part 1.2.	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s), but~~ did not implement the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~applicable systems as specified in ~~Requirement R1~~ Part 1.1, and did not implement the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~applicable systems as specified in ~~Requirement R1~~ Part 1.2; OR

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td></td><td>The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in ~~the requirement.~~Requirement R2.</td></tr>
<tr><td>R3.</td><td>The Responsible Entity ~~reviewed~~exceeded 15 calendar months by reviewing and ~~obtained~~obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than 15 calendar months but less than or equal to 16~~in the 16th calendar ~~months~~month since the previous review ~~as specified in the Requirement~~.</td><td>The Responsible Entity ~~reviewed~~exceeded the 15 calendar months by reviewing and ~~obtained~~obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than 16 calendar months but less than or equal to 17~~in the 17th calendar ~~months~~month since the previous review ~~as specified in the Requirement~~.</td><td>The Responsible Entity ~~reviewed~~exceeded 15 calendar months by reviewing and ~~obtained~~obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than 17 calendar months but less than or equal to 18~~in the 18th calendar ~~months~~month since the previous review ~~as specified in the Requirement~~.</td><td>The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review ~~as specified in the Requirement.~~.</td></tr>
</table>

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan ~~for Project 2019-03~~”

- CIP-013-~~2~~3 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	
2	3/18/2021	FERC Order approving CIP-013-2. Docket No. RD21-2-000.	
2	4/5/2021	Effective Date	10/1/2022
3	TBD	Virtualization Modifications	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-12

Definitions
Clean

CIP Definitions

Project 2016-02 Modifications to CIP Standards | Final Draft

The standard drafting team (SDT) is seeking comment on the following new or modified terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised Definition
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the Reliable Operation of the Bulk Electric System (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS) **Update is Acronym only.**	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	
BES Cyber System Information	Information about the BES Cyber System that could be	Information about the BES Cyber System (BCS) that

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
(BCSI)	used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	could be used to gain unauthorized access or pose a security threat to the BCS. BES Cyber System Information (BCSI) does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BCS, such as, but not limited to, device names, individual IP addresses without context, Electronic Security Perimeter names, or policy statements. Examples of BCSI may include, but are not limited to, security procedures or security information about BCS, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BCS.
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Cyber Security Standards.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.	Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: • For a high or medium impact BES Cyber System (BCS), compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring Systems; or (4) Shared Cyber Infrastructure; or • Disrupts or attempts to disrupt the operation of a BCS.
Cyber System ***New Definition***		One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	Cyber System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) (ESP) or BES Cyber Systems (BCS), including those not protected by an ESP used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	An electronic policy enforcement point or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable	The ability to access a BES Cyber System through its Electronic Security Perimeter via a bi-directional routable protocol connection.

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
	protocol connection.	
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated electronic access by a person using a bi-directional routable protocol: • To a Cyber System protected by an Electronic Security Perimeter(s) (ESP); • That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or • To a Management Interface. Interactive Remote Access does not include: • Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or • System-to-system process communication.
Intermediate System	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
Management Interface ***New Definition***		An administrative interface that: • Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; • Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or • Configures an Electronic Access Point.
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers	Cyber Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	One or more Cyber Assets or Virtual Cyber Assets (VCA) that: • Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or • Share CPU resources or memory resources with any part of the BCS, excluding VCA that are being

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
		actively remediated in an environment that isolates routable connectivity from BCS; Excluding Transient Cyber Assets.
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure (SCI), (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, SCI, a network protected by an Electronic Security Perimeter, or a Protected Cyber Asset.
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	A Cyber Security Incident that compromised or disrupted: • A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity; • An Electronic Security Perimeter of a high or medium impact BCS; • An Electronic Access Control or Monitoring Systems of a high or medium impact BCS; or • Shared Cyber Infrastructure supporting a BCS.
Shared Cyber Infrastructure (SCI) ***New Definition***		One or more programmable electronic devices, including the software that shares the devices' resources, that: • Hosts one or more Virtual Cyber Assets (VCA)

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
		included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or • Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization. SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset,	A Cyber Asset or Virtual Cyber Asset (VCA) that is: 1. Capable of transmitting or transferring executable code; 2. Not included in a BES Cyber System (BCS); 3. Not a Protected Cyber Asset (PCA) associated with high or medium impact BCS; and 4. Connected for 30 consecutive calendar days or less: • On a network protected by an Electronic Security Perimeter containing high or medium impact BCS; or

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
	• network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	• Directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a: ▪ BES Cyber Asset; ▪ Shared Cyber Infrastructure; or ▪ PCA associated with high or medium impact BCS. Virtual machines hosted on a physical Transient Cyber Asset (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Virtual Cyber Asset (VCA) ***New Definition***		A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include: • Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems; • Dormant file-based images that contain operating

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
		systems or firmware; or • SCI or Cyber Assets that host VCAs. Application containers are considered software of VCAs or Cyber Assets.

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit A-12

Definitions
Redline

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards | Final Draft

The standard drafting team (SDT) is seeking comment on the following new or modified terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the ~~reliable operation~~Reliable Operation of the Bulk Electric System~~.~~ (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS) **Update is Acronym only.**	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	
BES Cyber System Information	Information about the BES Cyber System that could be	Information about the BES Cyber System (BCS) that

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
(BCSI)	used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	could be used to gain unauthorized access or pose a security threat to the ~~BES Cyber System.~~BCS. BES Cyber System Information (BCSI) does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to ~~BES Cyber Systems~~BCS, such as, but not limited to, device names, individual IP addresses without context, ~~ESP~~Electronic Security Perimeter names, or policy statements. Examples of ~~BES Cyber System Information~~BCSI may include, but are not limited to, security procedures or security information about ~~BES~~BCS, Shared Cyber ~~Systems~~Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the ~~BES Cyber System~~BCS.
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC ~~CIP~~Critical Infrastructure Protection Cyber Security Standards~~, CIP-002 through CIP-011.~~.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.	Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of

Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved
		Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: ~~-~~For a high or medium impact BES Cyber System~~,~~ (BCS), compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, ~~or~~ (3) an Electronic Access Control or • Monitoring ~~System~~Systems; or (4) Shared Cyber Infrastructure; or • ~~-~~Disrupts or attempts to disrupt the operation of a ~~BES Cyber System~~BCS.
Cyber System ***New Definition***		One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	Cyber ~~Assets~~System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) ~~or BES Cyber Systems. This includes Intermediate Systems.~~(ESP) or BES Cyber Systems (BCS), including those not protected by an ESP used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic	~~A~~An electronic policy enforcement point or a Cyber Asset interface on an Electronic ~~Security Perimeter~~Access Control or Monitoring Systems that ~~allows~~controls routable communication ~~between~~to

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
	Security Perimeter.	and from one or more BES Cyber Systems or their associated Protected Cyber Assets~~ outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.~~.
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System ~~from a Cyber Asset that is outside of its associated~~through its Electronic Security Perimeter via a bi-directional routable protocol connection.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol~~.~~; or a logical boundary defined by one or more Electronic Access Points.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated electronic access by a person ~~employing a remote access client or other remote access technology~~ using a bi-directional routable protocol~~. Remote access originates from a Cyber Asset that is not an Intermediate~~ : • To a Cyber System ~~and not located within any of the Responsible Entity's~~ protected by an Electronic Security Perimeter(s) ~~or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1)~~ (ESP); • That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber ~~Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by~~

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
		~~employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants.~~ System; or • To a Management Interface. Interactive ~~remote access~~ Remote Access does not include~~ system~~: • Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or • System-to-system process ~~communications~~communication.
Intermediate System	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	~~A Cyber Asset~~One or ~~collection of Cyber Assets performing access control~~more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.~~ The Intermediate System must not be located inside the Electronic Security Perimeter.~~
Management Interface ***New Definition***		An administrative interface that: • Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; • Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system;

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
		or • Configures an Electronic Access Point.
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers	Cyber ~~Assets~~Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	One or more Cyber Assets ~~connected using a routable protocol within~~ or ~~on~~Virtual Cyber Assets (VCA) that: • Are protected by an Electronic Security Perimeter ~~that is~~(ESP) but are not part of the highest impact BES Cyber System ~~within~~(BCS) protected by the same ~~Electronic Security Perimeter. The impact rating~~ESP; or • Share CPU resources or memory resources with any part of ~~Protected Cyber Assets is equal to~~ the ~~highest rated BES~~BCS, excluding VCA that are being actively remediated in an environment that isolates routable connectivity from BCS;

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
		Excluding Transient Cyber ~~System in the same ESP.~~Assets.
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets~~,~~ or Shared Cyber Infrastructure (SCI), (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, SCI, a network ~~within~~protected by an ~~ESP~~Electronic Security Perimeter, or a Protected Cyber Asset. ~~Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	A Cyber Security Incident that compromised or disrupted: • ~~-~~A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity; • ~~-~~An Electronic Security Perimeter of a high or medium impact ~~BES Cyber System; or~~BCS; • ~~-~~An Electronic Access Control or Monitoring ~~System~~Systems of a high or medium impact ~~BES~~BCS; or • Shared Cyber ~~System~~Infrastructure supporting a BCS.
Shared Cyber Infrastructure (SCI) ***New Definition***		One or more programmable electronic devices, including the software that shares the devices'

Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved
		resources, that: • Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or • Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization. SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30	A Cyber Asset or Virtual Cyber Asset (VCA) that is: 1. ~~capable~~Capable of transmitting or transferring executable code~~,~~; 2. ~~not~~Not included in a BES Cyber System~~,~~ (BCS); 3. ~~not~~Not a Protected Cyber Asset (PCA) associated with high or medium impact ~~BES Cyber Systems,~~BCS; and 4. ~~directly connected~~Connected for 30 consecutive calendar days or less:

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
	consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	• On a network protected by an Electronic Security Perimeter containing high or medium impact BCS; or • Directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) ~~for 30 consecutive calendar days or less to a:~~to a: ▪ BES Cyber Asset~~,~~; ~~• network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or~~ ▪ Shared Cyber Infrastructure; or ▪ PCA associated with high or medium impact ~~BES Cyber Systems~~BCS. ~~Examples of~~ Virtual machines hosted on a physical Transient Cyber ~~Assets~~Asset (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Virtual Cyber Asset (VCA) ***New Definition***		A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System;

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
		Protected Cyber Asset; or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include: • Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems; • Dormant file-based images that contain operating systems or firmware; or • SCI or Cyber Assets that host VCAs. Application containers are considered software of VCAs or Cyber Assets.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards

Applicable Standard(s)

- Reliability Standard CIP-002-7 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-10 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-8 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-8 – Cyber Security – BES Cyber System Logical Isolation
- Reliability Standard CIP-006-7 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-7 – Cyber Security – System Security Management
- Reliability Standard CIP-008-7 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-5 – Cyber Security – Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-4 – Cyber Security – Information Protection
- Reliability Standard CIP-013-3 – Cyber Security – Supply Chain Risk Management
- Proposed new or modified terms listed in the "CIP Definitions Project 2016-02 Modifications to CIP Standards Final Draft".

  These standards and Definitions of Terms used in the versions listed above of the CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

  These standards and new and modified terms used in the standards above will be referenced as the "Revised CIP Standards and Definitions" within the Implementation Plan.

Requested Retirement(s)

- Reliability Standard CIP-002-5.1a – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-9 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-7 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)
- Reliability Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-6 – Cyber Security – System Security Management
- Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning

- Reliability Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-3 – Cyber Security – Information Protection
- Reliability Standard CIP-013-2 – Cyber Security – Supply Chain Risk Management

These standards and definitions used in the versions listed above will be referenced as the “Requested CIP Retired Standards” within the Implementation Plan.

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard(s) become effective:

- BES Cyber Asset (BCA)
- BES Cyber System (BCS)
- BES Cyber System Information (BCSI)
- CIP Senior Manager
- Cyber Assets
- Cyber Security Incident
- Cyber System
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate System
- Management Interface
- Physical Access Control Systems (PACS)
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Removable Media
- Reportable Cyber Security Incident
- Shared Cyber Infrastructure (SCI)
- Transient Cyber Asset (TCA)
- Virtual Cyber Asset (VCA)

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions. The intent of the Compliance Dates for Early Adoption of Revised CIP Standards and Definitions section is to permit Responsible Entities the option to comply with the Revised CIP Standards and Definitions prior to the Effective Date. While the Revised CIP Standards and Definitions are designed to be backwards compatible with perimeter-based security, some Responsible Entities may elect to comply early to leverage different security options associated with zero trust architecture.

Effective Date and Phased-in Compliance Dates

The Effective Dates for the Revised CIP Standards and Definitions are provided below. As noted in the General Considerations section above, the standard drafting team determined to clarify initial performance of periodic requirements and permit Responsible Entities to comply with the Revised CIP Standards and Definitions prior to the effective date. These provisions are also provided below.

Revised CIP Standards and Definitions

Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the later of: (1) April 1, 2026; or (2) the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority’s order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the date the Revised CIP Standards and Definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

---

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards.

Compliance Dates for Early Adoption of Revised CIP Standards and Definitions

A Responsible Entity may elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. In such a case, the Responsible Entity shall select one of the following Early Adoption Dates and shall notify the applicable Regional Entities of their selected Early Adoption Date within fifteen (15) calendar days after their selected Early Adoption Date:

Early Adoption Date
Option 1: First day of the first calendar quarter that is six (6) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 2: First day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 3: First day of the first calendar quarter that is eighteen (18) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions

Responsible Entities must comply with applicable Requested CIP Retired Standards until their selected Early Adoption Date. All Responsible Entities, regardless of whether or not they selected an Early Adoption Date, must comply with the Revised CIP Standards and Definitions by the Effective Date.

Planned or Unplanned Changes

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-7, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-7, Attachment 1, criteria.

For unplanned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirement not applicable to Medium impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Retirement Date

Requested CIP Retired Standards

The Requested CIP Retired Standards shall be retired immediately prior to the effective date of the Revised CIP Standards and Definitions in the particular jurisdiction in which the Revised CIP Standards and Definitions are becoming effective.

Exhibit C

Order No. 672 Criteria

EXHIBIT C

Order No. 672 Criteria

In Order No. 672,[1] the Commission identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The discussion below identifies these factors and explains how the proposed Reliability Standards have met or exceeded the criteria.

1. Proposed Reliability Standards must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve that goal.[2]

The proposed Reliability Standards would advance the reliability of the Bulk-Power System ("BPS") through the use of security objectives that help transform the CIP Reliability Standards into a framework that can support cyber security of the grid now and into the future. The proposed CIP Reliability Standards and associated definitions improve upon the currently effective cyber security CIP Reliability Standards by facilitating the use of security models enabled through virtualized technologies while also permitting Responsible Entities with more "traditional" architecture to continue with their current configurations. The proposed standards do so by leveraging "security objectives" to focus requirements on the essential elements a

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006) [hereinafter Order No. 672].

[2] *See* Order No. 672, *supra* note 1, at P 321 ("The proposed Reliability Standard must address a reliability concern that falls within the requirements of section 215 of the FPA. That is, it must provide for the reliable operation of Bulk-Power System facilities. It may not extend beyond reliable operation of such facilities or apply to other facilities. Such facilities include all those necessary for operating an interconnected electric energy transmission network, or any portion of that network, including control systems. The proposed Reliability Standard may apply to any design of planned additions or modifications of such facilities that is necessary to provide for reliable operation. It may also apply to Cybersecurity protection.").

See Order No. 672, *supra* note 1, at P 324 ("The proposed Reliability Standard must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve this goal. Although any person may propose a topic for a Reliability Standard to the ERO, in the ERO's process, the specific proposed Reliability Standard should be developed initially by persons within the electric power industry and community with a high level of technical expertise and be based on sound technical and engineering criteria. It should be based on actual data and lessons learned from past operating incidents, where appropriate. The process for ERO approval of a proposed Reliability Standard should be fair and open to all interested persons.").

Responsible Entity must meet to support reliability. Additionally, the use of security objectives helps to set up the framework to adapt to newer technologies and innovative security models as they become part of Responsible Entities' choices to support their systems.

The proposed Reliability Standards are designed to achieve a specific reliability goal (i.e., protect against Bulk Electric System ("BES") Cyber Systems' impact to the Bulk Electric System if rendered unavailable, degraded, or misused), and contain technically sound means to achieve that goal through requirements based on good cyber security practices and security objectives.

2. Proposed Reliability Standards must be applicable only to users, owners, and operators of the bulk power system, and must be clear and unambiguous as to what is required and who is required to comply.[3]

The proposed Reliability Standards are clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672. The proposed Reliability Standards apply to Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners. The proposed Reliability Standards clearly articulate the actions that such entities must take to comply with the standards.

3. A proposed Reliability Standard must include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation.[4]

The Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") for the proposed Reliability Standard comport with NERC and Commission guidelines related to their assignment, as discussed further in **Exhibit F**. The assignment of the severity level for each VSL

---

[3] *See* Order No. 672, *supra* note 1, at P 322 ("The proposed Reliability Standard may impose a requirement on any user, owner, or operator of such facilities, but not on others.").

See Order No. 672, *supra* note 1, at P 325 ("The proposed Reliability Standard should be clear and unambiguous regarding what is required and who is required to comply. Users, owners, and operators of the Bulk-Power System must know what they are required to do to maintain reliability.").

[4] *See* Order No. 672, *supra* note 1, at P 326 ("The possible consequences, including range of possible penalties, for violating a proposed Reliability Standard should be clear and understandable by those who must comply.").

is consistent with the corresponding requirement, and the VSLs should ensure uniformity and consistency in the determination of penalties. The VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations. For these reasons, the proposed Reliability Standards include clear and understandable consequences in accordance with Order No. 672.

4. A proposed Reliability Standard must identify clear and objective criteria or measures for compliance, so that it can be enforced in a consistent and non-preferential manner.[5]

The proposed Reliability Standards contain measures that support each requirement by clearly identifying what is required and how the requirement will be enforced. These measures help provide clarity regarding how the requirements would be enforced and help ensure that the requirements would be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.

5. Proposed Reliability Standards should achieve a reliability goal effectively and efficiently, but do not necessarily have to reflect "best practices" without regard to implementation cost or historical regional infrastructure design.[6]

The proposed Reliability Standards achieve their reliability goals effectively and efficiently in accordance with Order No. 672. Through the use of security objectives in the proposed Reliability Standards, the proposed requirements alert Responsible Entities to their obligations but also permit Responsible Entities to choose various security models that best fit their organization's configurations while meeting the objective of the requirement.

6. Proposed Reliability Standards cannot be "lowest common denominator," i.e., cannot reflect a compromise that does not adequately protect Bulk-Power System reliability.

---

[5] *See* Order No. 672, *supra* note 1, at P 327 ("There should be a clear criterion or measure of whether an entity is in compliance with a proposed Reliability Standard. It should contain or be accompanied by an objective measure of compliance so that it can be enforced and so that enforcement can be applied in a consistent and non-preferential manner.").

[6] *See* Order No. 672, *supra* note 1, at P 328 ("The proposed Reliability Standard does not necessarily have to reflect the optimal method, or 'best practice,' for achieving its reliability goal without regard to implementation cost or historical regional infrastructure design. It should however achieve its reliability goal effectively and efficiently.").

Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.[7]

The proposed Reliability Standards do not reflect a "lowest common denominator" approach. The proposed Reliability Standards would further advance the reliable operation of the Bulk-Power System by focusing Responsible Entities on the underlying goal of the requirement rather than a prescribed topology or the "lowest common denominator" topology.

7. Proposed Reliability Standards must be designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one geographic area or regional model. It should take into account regional variations in the organization and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.[8]

The proposed Reliability Standards would apply consistently throughout North America and do not favor one geographic area or regional model. The proposed Reliability Standards would provide sufficient flexibility to accommodate regional/geographic variations, including climate, generation type, market issues, state rules, and other considerations.

---

[7] *See* Order No. 672, *supra* note 1, at P 329 ("The proposed Reliability Standard must not simply reflect a compromise in the ERO's Reliability Standard development process based on the least effective North American practice—the so-called 'lowest common denominator'—if such practice does not adequately protect Bulk-Power System reliability. Although the Commission will give due weight to the technical expertise of the ERO, we will not hesitate to remand a proposed Reliability Standard if we are convinced it is not adequate to protect reliability.").

See Order No. 672, *supra* note 1, at P 330 ("A proposed Reliability Standard may take into account the size of the entity that must comply with the Reliability Standard and the cost to those entities of implementing the proposed Reliability Standard. However, the ERO should not propose a 'lowest common denominator' Reliability Standard that would achieve less than excellence in operating system reliability solely to protect against reasonable expenses for supporting this vital national infrastructure. For example, a small owner or operator of the Bulk-Power System must bear the cost of complying with each Reliability Standard that applies to it.").

[8] *See* Order No. 672, *supra* note 1, at P 331 ("A proposed Reliability Standard should be designed to apply throughout the interconnected North American Bulk-Power System, to the maximum extent this is achievable with a single Reliability Standard. The proposed Reliability Standard should not be based on a single geographic or regional model but should take into account geographic variations in grid characteristics, terrain, weather, and other such factors; it should also take into account regional variations in the organizational and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.").

8. Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.[9]

The proposed Reliability Standards would have no undue negative effect on competition and would not unreasonably restrict the available transmission capacity or limit the use of the BPS in a preferential manner. The proposed standards would require the same performance from each of the applicable entities.

9. The implementation time for the proposed Reliability Standard is reasonable.[10]

The proposed implementation plan for the proposed Reliability Standards is just and reasonable and appropriately balances the urgency in the need to implement the standards against the reasonableness of the time allowed for those who must comply to develop necessary procedures or other relevant capability. The proposed implementation plan is discussed in detail in the main petition and is attached as **Exhibit B.**

10. The Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[11]

The proposed Reliability Standards were developed in accordance with NERC's Commission-approved processes for developing and approving Reliability Standards. **Exhibit G**

---

[9] *See* Order No. 672, *supra* note 1, at P 332 ("As directed by section 215 of the FPA, the Commission itself will give special attention to the effect of a proposed Reliability Standard on competition. The ERO should attempt to develop a proposed Reliability Standard that has no undue negative effect on competition. Among other possible considerations, a proposed Reliability Standard should not unreasonably restrict available transmission capability on the Bulk-Power System beyond any restriction necessary for reliability and should not limit use of the Bulk-Power System in an unduly preferential manner. It should not create an undue advantage for one competitor over another.").

[10] *See* Order No. 672, *supra* note 1, at P 333 ("In considering whether a proposed Reliability Standard is just and reasonable, the Commission will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability.").

[11] *See* Order No. 672, *supra* note 1, at P 334 ("Further, in considering whether a proposed Reliability Standard meets the legal standard of review, we will entertain comments about whether the ERO implemented its Commission-approved Reliability Standard development process for the development of the particular proposed Reliability Standard in a proper manner, especially whether the process was open and fair. However, we caution that we will not be sympathetic to arguments by interested parties that choose, for whatever reason, not to participate in the ERO's

includes a summary of the Reliability Standards development proceedings, and details the processes followed to develop the proposed Reliability Standards. These processes included, among other things, comment periods, pre-ballot review periods, and balloting periods. Additionally, meetings of the standard drafting team were properly noticed and open to the public.

11. NERC must explain any balancing of vital public interests in the development of proposed Reliability Standards.[12]

NERC has identified no competing public interests regarding the request for approval of these proposed Reliability Standards. No comments were received that indicated that the proposed Reliability Standards conflict with other vital public interests.

12. Proposed Reliability Standards must consider any other appropriate factors.[13]

No other negative factors relevant to whether the proposed Reliability Standards are just and reasonable were identified.

Reliability Standard development process if it is conducted in good faith in accordance with the procedures approved by the Commission.").

[12] *See* Order No. 672, *supra* note 1, at P 335 ("Finally, we understand that at times development of a proposed Reliability Standard may require that a particular reliability goal must be balanced against other vital public interests, such as environmental, social and other goals. We expect the ERO to explain any such balancing in its application for approval of a proposed Reliability Standard.").

[13] *See* Order No. 672, *supra* note 1, at P 323 ("In considering whether a proposed Reliability Standard is just and reasonable, we will consider the following general factors, as well as other factors that are appropriate for the particular Reliability Standard proposed.").

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit D

Virtualization and Future Technologies: The Case for Change White Paper

Virtualization and Future Technologies

Project 2016-02 Standards Drafting Team: The Case for Change

April 2019

Table of Contents

Executive Summary

What the interconnected power grid does for Bulk Electric System (BES) reliability, virtualization does for the computing infrastructure supporting vital control systems. Individual utilities interconnected their power systems to form a power grid to share spare capacity for meeting demand peaks and surviving contingencies such as generating unit and transmission line outages. Virtualization connects processors, networks, and storage into ‘computing grids’ that allow our vital systems and applications to meet peak demands and survive outages of individual components.

This is accomplished by abstracting servers, networks, and storage into virtual or logical resources that can be independent of specific underlying hardware such as individual processors, circuits, and disks. A control system and its underlying operating system become a virtual machine and can move to any available hardware. This greatly increases reliability and resiliency of our control systems that support BES reliability.

Virtualization technologies also allow enhanced cyber security controls and the ability to move access controls from the edge of our networks to much deeper inside of them. This is analogous to having generation close to load centers to reduce the susceptibility to outages. These newer security controls allow us to provide tighter security by moving access controls from an outer perimeter closer to the actual code performing reliability tasks.

Virtualization and advanced technology are challenging the way we characterize the Critical Infrastructure Protection (CIP) standards’ objectives and how we develop technical requirements. Use of virtualization and advanced technology can provide benefits for implementing both operational and security enhancements to a system. The goal is to require technology-enforced controls as alternatives to the current prescriptive requirements like those requiring a physically structured architecture, without forcing the use of the new technology. The existing standards with their prescriptive language limit the ability to take full advantage of the new technologies. The Project 2016-02 Modifications to CIP Standards Standard Drafting Team (SDT) is drafting new requirements to support virtualization capabilities. This leaves Responsible Entities with the option to maintain a non-virtualized environment and use backward compatibility to preserve current CIP investments and security postures.

This white paper represents the views of the SDT and presents a sampling of virtualization concepts. It explains, in the SDT’s opinion, how the use of these concepts is inhibited by some of the CIP standards’ definitions and requirements. It also introduces the SDT’s ideas on how to address these issues while maintaining compatibility with current state. The goal is to allow for the use of these technologies and newer security controls by removing prescribed “how’s” and replacing them with clear “what’s” that would allow both current state and these enhanced features.

Introduction

Note: The Project 2016-02 SDT developed this white paper to explain the need to change the cyber security CIP Reliability Standards. This white paper has not been approved or endorsed by NERC and is solely the views of the Project 2016-02 SDT.

In the history of the CIP standards, industry has seen many versions and changes. Some have been straightforward and almost self-explanatory. Others, complex and time-consuming to implement. Still others have been foundational, like the 'do-over' change from Versions 1 – 3 to Version 5. Not surprisingly, the prospect of another set of fairly major changes, this time involving virtualization sparks a great deal of industry concern. It raises valid questions about the timing and the drivers of those changes, and whether or not they are truly necessary. The white paper is designed to provide detailed answers to those questions from the viewpoint of the SDT. This introductory section provides a short, high level introduction to the white paper discussion on what brought about the SDT's focus on future revisions to the CIP standards to address virtualization.

Recognizing the continuing growth in technology innovation, many entities in the Electricity Sector have implemented virtualization as part of their CIP programs. Many of these same entities, however, have implemented this new technology without taking full advantage of virtualization's advanced capabilities. There are a number of reasons for this from the constraints of the current CIP architecture to the ongoing ambiguity around how new virtualization technology applies to CIP compliance. Some of those who are implementing virtualization are experiencing a great deal of uncertainty and difficulty around developing implementation strategies that will support compliance and achieve greater reliability and security.

These issues began coming to light following the NERC "Virtualization Summit" in 2015. Ultimately, the Version 5 Transition Advisory Group (V5TAG) heard about the industry concerns and determined that the issues around the standards and virtualization would be best addressed by a drafting team. The Project 2016-02 SDT was assigned the task to address the technological innovation in virtualization within the CIP standards.

The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards. The SDT's intent is to better position the CIP standards to be applicable to any future technological innovation. Leveraging the abstraction that virtualization provides will allow the industry to more readily adopt new technology and increase security posture. This paper presents the SDT's case for change to the NERC CIP standards that is needed to allow for the innovative security techniques and new concepts brought about by virtualization.

As virtualization has progressed, many of these types of issues cannot be addressed with Implementation Guidance. Documenting a possible way to implement a requirement is of great value, but Implementation Guidance cannot, for example, change current requirements so they do not prescribe a perimeter-based model, or allow remediation VLANs. It also cannot add new requirements that are needed for issues like management plane isolation or handling shared infrastructure. These new concepts and techniques require changes to the standards to make them viable and to clarify how they should be secured.

Chapter 1: Virtualization Benefits

The most basic concepts of CIP are essentially unchanged from the Urgent Action 1200 standard in 2003. The primary focus of those standards was the "critical cyber asset"; an "electronic device" such as a server, workstation, or relay as a physical object. It had an operating system, always on and performing its function, and communicating with other components over routable protocols. It was protected by traditional firewalls at the network edge looking at source and destination protocol addresses and ports as the only mechanism by which to make network access control decisions.

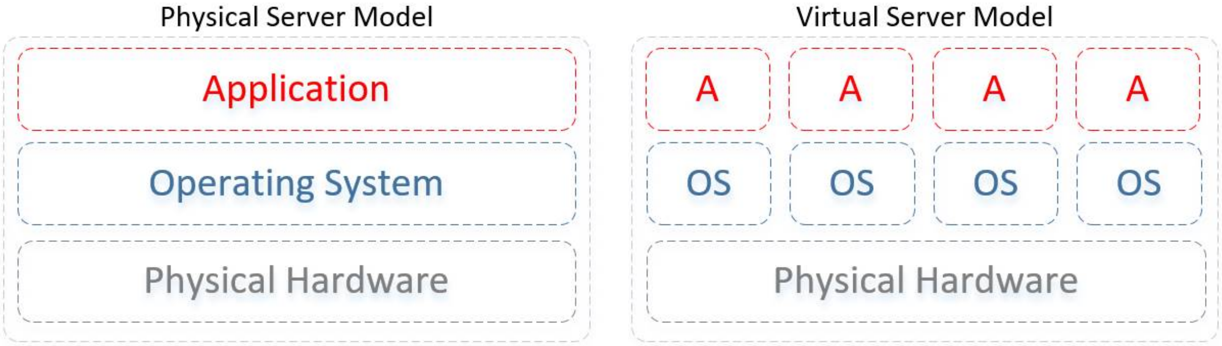


Figure 1

Today, virtualization has changed this scenario. With virtualization, physical devices are no longer the primary units of organization. An entire control system infrastructure can be virtualized (such as "software defined data centers") and only exist as logical constructs. An EMS database server may never exist as a discrete physical object. With containers (operating system emulation), there may not be a concrete tie between application logic and an operating system. Virtual machines can be created and destroyed dynamically and are neither always on, nor tied to specific hardware. Workloads may mirror their information for reliability purposes across great distances without using routable protocols. With micro-segmentation, network access control lists are now much more granular than IP addresses at a perimeter. They are enhanced by policy-based control templates enforcing access at a "user to workload" level throughout the system infrastructure. Electronic access control may no longer be based solely on routable protocol addresses or found only at an ESP boundary.

Benefits of Virtualization

Virtualization technologies bring many reliability benefits to BES Cyber Systems (BCS).

- Increased uptime, very fast recovery capability and flexible architecture that can instantly adapt to changing workloads.
- Virtualization allows for racks of CPUs, memory and disks to be tied together with high speed mesh networks and viewed simply as raw computing resources.
- If the workload on a particular virtual server is nearing capacity, the infrastructure orchestration system can create and configure an additional server on the fly, bring it online to help with the peak workload, and then destroy it when it is no longer needed.

- If a physical machine runs out of resources, the workload can be moved to another physical machine dynamically based upon relative load. When a virtual server or workstation is not in use, it is similar to a physical server that is powered off.
- This flexible and dynamic architecture also allows improved security controls such as those provided by micro-segmentation.
- Users can be granted access to specific workloads that can be placed dynamically throughout the infrastructure with managed access to provided services.

More secure, more reliable, cost effective technology solutions

New and innovative security capabilities continue to evolve to address current threats, particularly in virtualized environments. These capabilities can increase the security of hosted BES Cyber Systems. For example, *distributed firewalls* based on software defined access policies can enforce access controls at a much deeper level within the infrastructure to help prevent an attacker's lateral movement through the network. *Privileged introspection* allows security service such as anti-malware, to operate in a tamper-proof way outside of the instances they protect. *Zero trust models* allow communication to be protected end to end between individual processes across cyber assets without having to trust that devices in the path (such as all firewalls and switches) are configured correctly to protect the data. We'll consider each of these and other examples in more detail to show the benefits and the case for change in the CIP standards.

Chapter 2: Virtualization challenges in the NERC CIP Standards

Virtualization brings benefits to reliability and resiliency of our BES Cyber Systems. It also brings challenges with determining how some of the newer concepts fit within the framework of the NERC CIP standards. Some of these newer techniques and concepts are:

- Identification of Virtual Cyber Assets
- Distributed Firewalls vs. Perimeter models
- Zero Trust models
- Virtualized Firewall Interfaces
- Virtual Storage challenges
- Management Plane Isolation
- Privileged Introspection
- Remediation VLANs

Each of these topics will be covered in detail in the following sections.

Identification of Virtual Cyber Assets

One of the issues requiring change within the CIP standards is the need to clarify the treatment of virtual machines (VMs) under today's definitions. The foundational term Cyber Asset is defined as "Programmable electronic devices, including the hardware, software, and data in those devices." This definition, since it includes the hardware, does not fit with virtualized environments. A literal use of this foundational definition would mean a server hardware platform may be a BES Cyber System, the hypervisor software could be the "operating system", and all the virtual machines running on the hardware are applications or simply data. The CIP-007 requirements, most of which are aimed at an operating system instance, would not be applied to these virtual machines since they aren't hardware. This is referred to in the Figure 2 as the "Physical System w/Software Model."

To require that VM operating systems be classified correctly, the tie between a virtual machine and the hardware needs to be clarified. The standards and their associated definitions need to clearly support the "VM as a CA Model" (Virtual Machine as a Cyber Asset) as pictured in Figure 2. Here it is clear that the physical server hardware and the hypervisor are in scope and each VM is subject to requirements such as CIP-007.

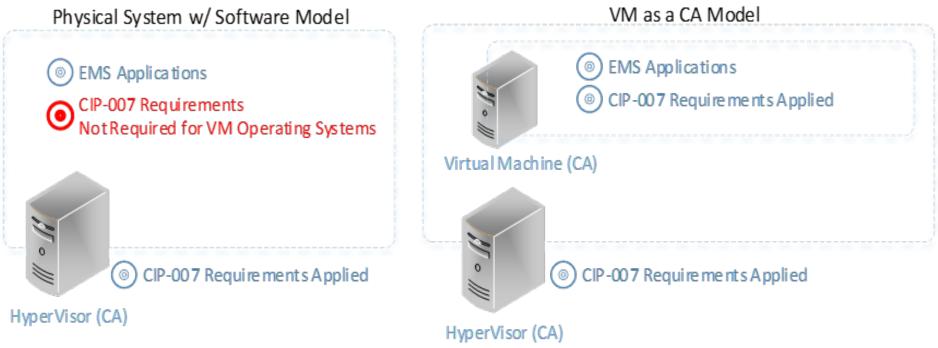


Figure 2

The Cyber Asset definition assumes a 1:1 relationship between a BES Cyber Asset and its hardware. Virtualization, however, breaks that concept because in some cases hundreds of virtual BES Cyber Assets can share a pool of hardware resources (compute, network, and storage). The outdated concepts need to be changed to recognize the one-to-many relationships that are now possible between a BES Cyber Asset, an instance of an operating system supporting applications, and the underlying hardware so it is clear how each is to be treated. There are three different types of asset classes involved in today's BES Cyber Systems:

- Self-contained devices that are composed of dedicated hardware, some form of operating system or firmware, and the application code. This is the traditional definition of a Cyber Asset and applies to things such as digital relays, RTUs, physical operator workstations and dedicated physical servers.
- Virtual "cyber assets" composed of an operating system and applications or containers minus any dedicated hardware. These types of assets are logical or virtual constructs by nature and exist only in memory or files. They can, however, appear from a network perspective the same as any other host.
- Shared Infrastructure consists of the hardware resource pools (compute, network, storage) and is shared by virtual cyber assets and can host numerous virtual cyber assets, networks, or storage locations.

The current CIP standards only recognize the first class and changes are needed to properly address the other two. This will allow BES Cyber Systems, which can be composed of all three asset classes, to be properly identified and classified and the proper requirements applied to each one.

Distributed Firewalls vs. Perimeter Models

Distributed firewalls based on software defined access policies can enforce access controls deeply within the infrastructure to help prevent an attacker's lateral movement through the network. The CIP standards (CIP-005) today require a perimeter-based model as shown in the left side of Figure 3. It has an Electronic Security Perimeter (ESP) as a logical border around a group of cyber assets, and defined interfaces (on a firewall for example) as an Electronic Access Point (EAP). This perimeter model is a prescriptive topology, and for many scenarios is still a valid way to perform network security. What may be prescribed, however, for a small network of similar cyber assets may not be ideal for a large network of virtualized BES Cyber Assets.

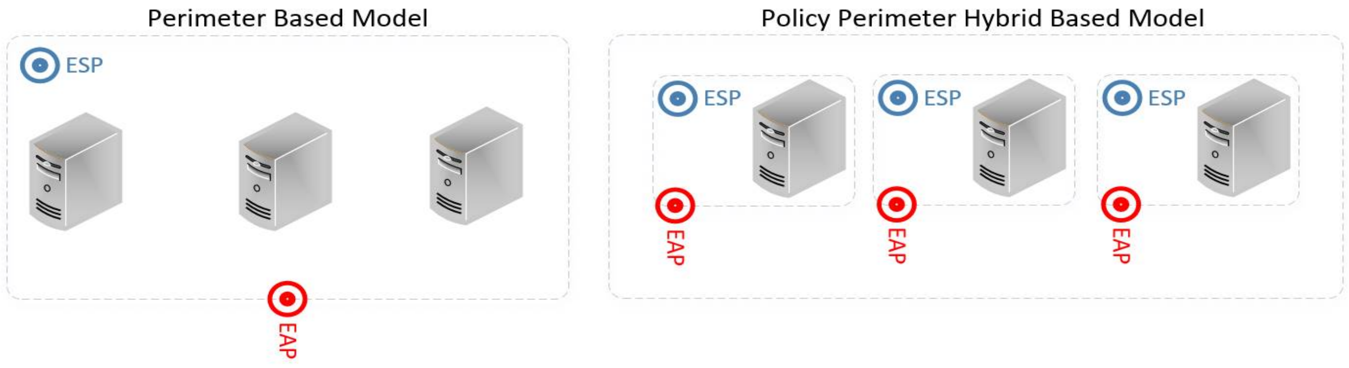


Figure 3

The issue is that network access is permitted or denied at the outer EAP "gate." Even if access is only needed to a single cyber asset inside the perimeter and a strict rule is instituted at the EAP "gate" to allow someone access to that single cyber asset, that control is implemented only at the gate. Once inside the perimeter, there are no network level access controls that would prevent hopping ("pivoting") from that cyber asset to all other cyber assets inside the perimeter. Attackers today depend upon this; if they can get a foothold on a single cyber asset inside a perimeter they can work over time to move laterally within the environment from there.

Virtualized environments, especially those of cloud providers that support tenants from various customers, had to be designed to implement new, more granular security techniques to not only mitigate this threat but to also keep customer's workloads totally isolated from one another. These new techniques are philosophically simple – every cyber asset is inside its own "perimeter" and the EAP "gates" are specific to each virtual cyber asset. This is shown on the right side of Figure 3 in the "Policy Perimeter Hybrid Based Model." In this model, network access is controlled at an individual cyber asset level and access to a single cyber asset gives you no additional access to any other cyber asset. An attacker's ability to move laterally or pivot in this environment is greatly reduced. These techniques are also configured at a *network access policy* level and the infrastructure dynamically implements it at various levels throughout the entire infrastructure. Even as these cyber assets move dynamically within the infrastructure, these access controls move with them. All of this, however, precludes the ability of administrators to provide a "list" of potentially hundreds or thousands of ESPs, EAPs, or the discrete rules per EAP. This is because it is all dynamically generated by the infrastructure to control access in accordance with a higher-level access policy.

These same techniques can be used to mitigate the same risks within virtualized CIP environments. The problem is that CIP requires the perimeter model with EAP "gates" as the only prescribed way to implement network level security. The SDT is planning to change the CIP standards and definitions in a way that does not *preclude* the perimeter based model, but also does not t *prescribe* that model as the only way. For example, the language in CIP-005 R1.2 "All External Routable Connectivity must be through an identified Electronic Access Point (EAP)." This creates an issue since historically this is a physical interface on a physical device. More current, virtualized architectures distribute the policy enforcement tasks to multiple devices and each of them validates that the network communications passing through it are permitted. The current standards do not align with these architectures because there is no single interface identified that is responsible for policy enforcement.

Identifying non-routable EAPs and the OSI Model

Related to the ESP issue, today's CIP Standards are limited to prescriptive topologies even as potentially more secure, reliable and cost-effective solutions are available. ESP's are defined today by the access provided at the network layer (OSI Layer 3) and are therefore limited to making access decisions based on routable protocol addresses. This method does not support security evaluation or compliance via security solutions at any of the other layers of the OSI model. This presents two issues:

- There may be network access into and out of the perimeter at different layers other than by a purely routable protocol that allow for things like high speed replication of data. This will be discussed further in the "Multi-Site Data Center Extensions (Super ESP)" section below.
- Virtualized environments have much more context and can enforce network access control at more granular levels in much better ways. These include by user, process, or certificate and are not limited to only a source/destination IP address of a routable protocol.

In many environments today, the perimeter model is sufficient and routable protocol addresses are all an entity has to make access control decisions. However, the standards should not prescribe this as the only way and should allow entities to use these more granular controls that may operate at other layers.

Zero Trust Models

The zero trust network model is a new and different way of thinking about network security. In most cases it can be implemented within the security model that an entity currently has deployed.

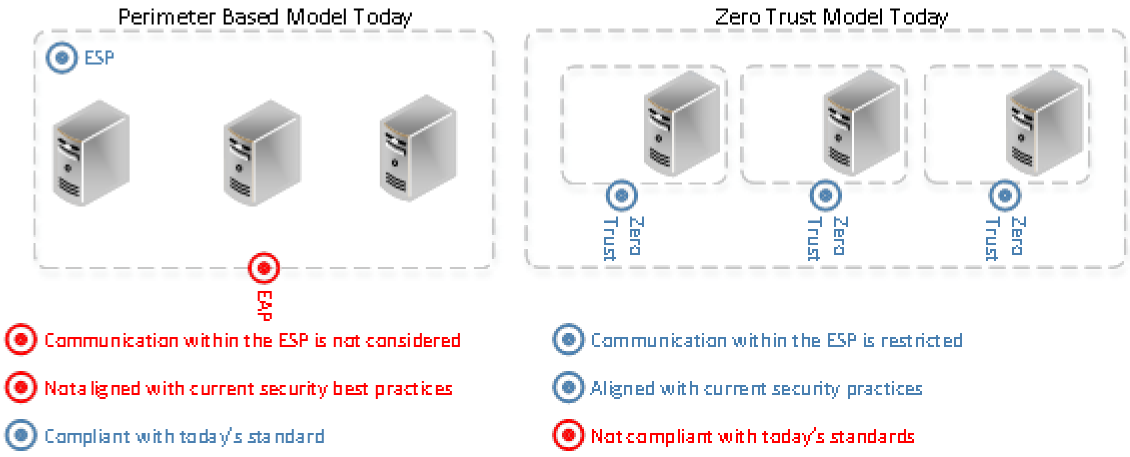


Figure 4

Most entities have a perimeter model deployed, which is what the current ESP model requires as in Figure 4. Traditionally, this consists of a firewall (or firewalls), with a single path into the network (EAP). This model protects the BES Cyber System indirectly, by protecting the network topology. This access point is protected by rules and policies that tell the firewall what kind of traffic to pass and what kind of traffic to stop. This model can be loosely compared to a gated community, where the fence is the firewall, and the gate and security guard are the access control.

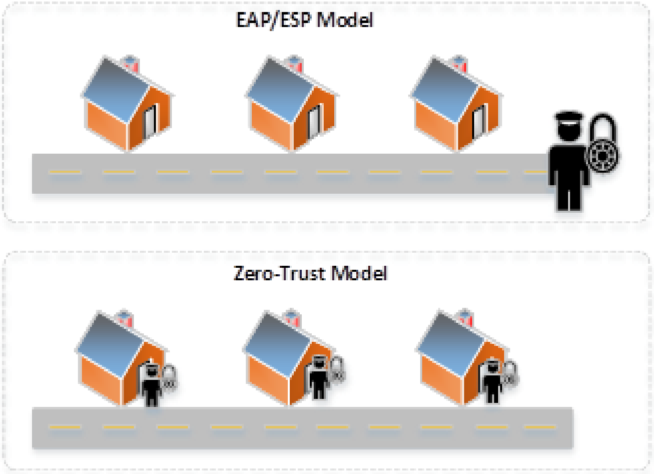


Figure 5

The overarching problem with this model is that if attackers should get past the firewalls and through the gate, they would have free rein throughout the network and could pose a serious threat to other BES Cyber Systems within the ESP.

A zero trust model brings the protection directly to the cyber asset or even to the process level. Using network policies, whitelisting, certificates, and other technologies, the ability of an intruder to move around is severely restricted. A zero trust model usually starts with simple items like restricting network traffic to the device except that which is necessary for it to perform its job function. It also restricts what logins can access the device. Finally, it introduces more complex ideas such as digitally signed executables, restrictions on what time a process can be started, and end to end encrypted traffic, even within the local network. This model protects the BES Cyber System directly by protecting the workloads, the devices and the topology. Unfortunately, this model is very difficult to describe using the current language constructs of the CIP requirements.

Referring to the gated community analogy in Figure 5, this would put a fence in every yard, a lock on every door and an alarm system in every house. This effectively isolates the intruder to the public areas of the neighborhood.

Virtualized Firewall Interfaces ('Firewall on a Stick')

As the use of network segmentation grows and firewalls are used to control traffic flows between the network segments, firewalls need higher densities of interfaces. To obtain these higher densities, products today rely on fewer physical ports and instead use virtualized network interfaces to emulate many physical interfaces. Some modern firewalls are service modules (a "firewall on a stick") installed in a switch or router where virtual interfaces are the only option to route traffic to and from the firewall as shown in Figure 6.

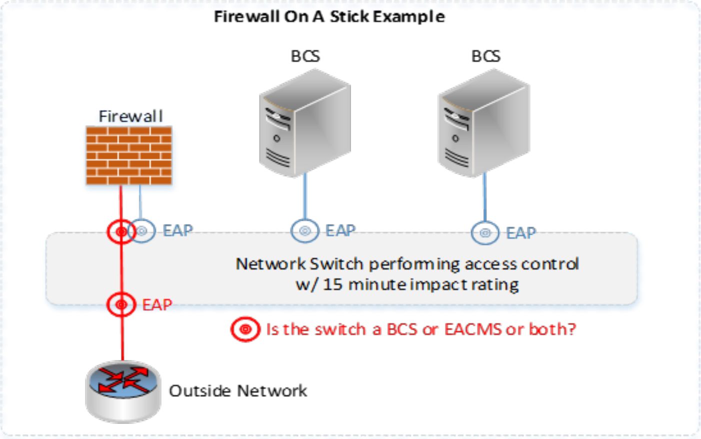


Figure 6

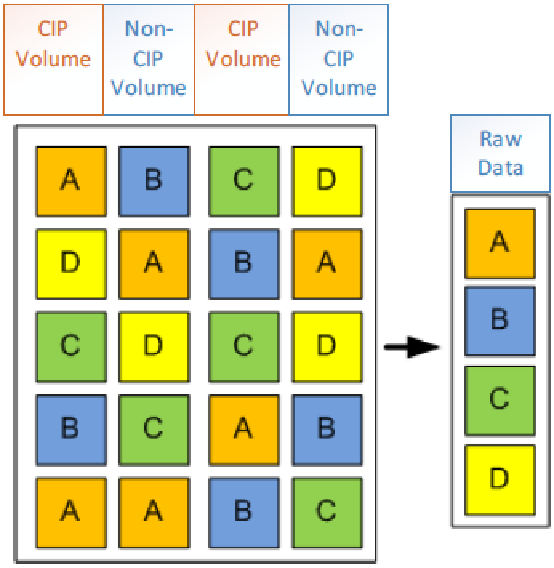
The CIP standards are ambiguous on how to properly identify these assets. If this were simply a network switch allowing two BES Cyber Systems to communicate with each other with a 15 minute impact if the switch is unavailable, then the switch itself is part of a BES Cyber System. In this example, the entity wanted to increase security of the communications between these two systems. To accomplish this, it put each BCS on its own network segment so it can filter all traffic between these two systems through a firewall. A "firewall on a stick" is installed in the switch and the ports on the switch are divided into virtual networks so the traffic between different segments is directed to the firewall and controlled. Since the firewall either has no physical interface or may use its few physical interfaces for redundancy, the outside network must connect to the same switch and that port is configured to the "outside" interface of the firewall. All communications to and from the outside network and between the two BCS are all controlled via the firewall. The entity has increased the security of these systems, but it is now undecided on how to identify the cyber assets in this scenario. As one example, are all the network switch ports now EAPs on an EACMS, or is this switch still just a part of the BCS? As access control is pushed deeper into networks as in this example, the current paradigms are ambiguous. The answer may lie in identifying new asset classes and developing new objective requirements that do not include prescriptive network topology assumptions. Trunks and sub-interfaces are common network technologies to aggregate data streams and better utilize limited physical interfaces[1].

---

[1] Trunking is the use of a single link to aggregate multiple data streams. This technology is widely used in networking and telecommunications. Sub-interfaces allow for multiple LAN segments to share a common physical interface.

Virtual Storage Challenges

As we move to virtual storage, there are issues with some of today's CIP concepts. For example, the CIP-011-2, requirement R2 restricts unauthorized access to BES Cyber System Information on systems meant for reuse outside of the CIP environment or systems meant for disposal. This causes a challenge for virtualized infrastructure. Today, when disposing of a physical medium or high impact BES Cyber Asset, access to BCSI can be restricted by sanitizing or destroying the media associated with the physical asset. If storage media is provided from a Storage Area Network (SAN) or Network Attached Storage (NAS) array, there may be no easy way to identify the specific drives where the data might have been stored. Additionally, there is no significant benefit to pulling drives from an array to sanitize or destroy them if there is another way to manage this media.



Deduplication Example

Figure 7

To extend this challenge further, many SAN and NAS environments can de-duplicate and move data to various storage tiers within the array to optimize access times and reduce latency. This process analyzes the data in small enough chunks to create single instances of data that are used within multiple volumes that may be assigned to any number of devices. The chunks with the highest access rates are then placed on fast storage media because the data is constantly referenced. This effectively causes data re-use if storage media is shared between CIP and Non-CIP assets even when the information contained within these de-duplicated chunks is not readily retrievable individually.

That was one example. The CIP standards were built on a paradigm of disk storage being physical disks dedicated to a Cyber Asset. Updates to the standards are needed to reflect the realities of virtual storage technologies that are in use today.

Management Plane Isolation

Because virtualized servers, networks, switches, firewalls, and storage are logical constructs, controlling access and communications to the management plane of these systems is imperative. Access to the management plane (interface/console/etc.) allows a user to create, modify, or delete these objects or entire infrastructures from one place, or move objects from one zone or network to another. Administrative level or "management plane" access to the hypervisors is therefore absolutely critical to the security and reliability of the hosted systems. These types of access must be brought into the scope of CIP standards if hosting BES Cyber Systems and will require changes to the CIP standards.

Another challenge of the perimeter model is it can drive less secure topologies in order to provide clear adherence to the perimeter model. In Figure 8 below on the right is the desired separation between the management plane of a virtualized environment and the production or "data plane". The management port of the BCA is connected to a switch on the management network. The production network switch is connected to the network interface on the BCA. This creates two different network paths to the BCA: one for normal production traffic and a separate network path with separate access controls for administrative or management plane access. It is unclear, however, if the BCA has now created two ESP's with two EAPs, and whether or not it is now an EACMS. It is not functioning as an EACMS, but from the topology it appears as one. The prescriptive CIP model may create a temptation to place the management interface into the production ESP as in the picture on the left. This is very clear from a CIP standard adherence perspective but is the less secure choice.

Figure 8

Privileged Introspection

Privileged introspection allows security services, such as malware detection, to be performed outside of the operating system and applications it is protecting in a tamper-proof way. Previously, malware that could gain elevated privileges on a cyber asset could then disable security services such as anti-virus solutions running on the same OS. Virtualized environments, however, can allow privileged introspection where anti-virus or application whitelisting services run as part of the hypervisor; outside of the operating system they are protecting so malware with elevated privileges inside the OS cannot reach them. Another benefit of privileged introspection is it allows integration with distributed firewalls because it can inspect network traffic entering or leaving virtual machines and make decisions with vastly more context. For example, these firewalls can control access not simply at a network address level (IP source/destination) but down to the level of a process with a particular certificate.

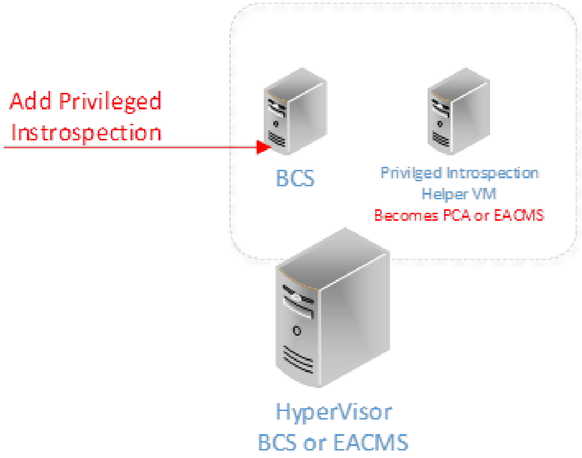


Figure 9

Even though the current CIP-007 R3 is already written at a security objective level and can work with privileged introspection, there can still be CIP standards issues brought into play. If this functionality uses "helper VMs", it is not clear how to identify and classify these under the current CIP standards. Since the status of malware detection is now outside the VM's, it requires grouping the VM's protected by privileged introspection into a particular BES Cyber System.

Remediation VLANs

As another example of the need for change in the CIP standards brought about by new virtualization technologies, CIP-010 R3.3 states, "Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset..." This is a valid requirement that cyber assets be in a CIP compliant state before being added to a production CIP environment. The issue is that this is written with the idea that an entity's new cyber asset is a separate physical asset it can configure in a compliant state prior to it being placed in a "production environment" and connected to a production network.

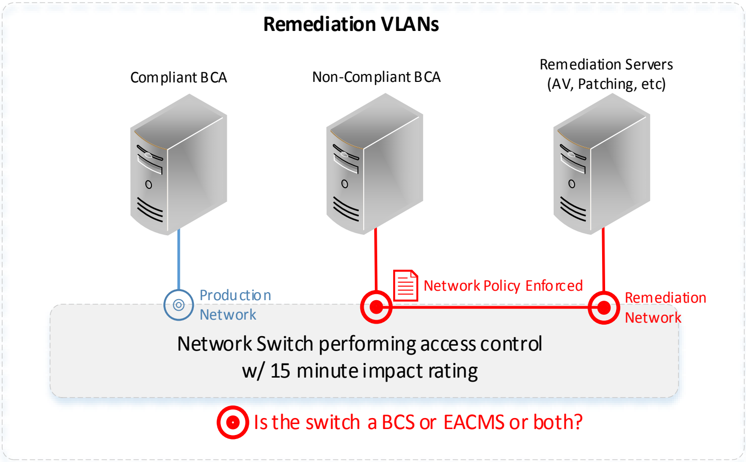


Figure 10

Virtualized environments, however, allow for a concept known as remediation VLANs. When a new cyber asset, such as a server or operator workstation is instantiated from an image, it is already "in" a production environment. However, it is brought up in a remediation VLAN where its network visibility is restricted to those services (patching, anti-virus updates, etc.) that it needs to assess vulnerabilities, update itself, and become compliant. Only after it is fully compliant with policy, can it be moved to a production VLAN where it has the full network visibility. Should this virtual machine become non-compliant with the network policy, it is moved back to the remediation VLAN to be made compliant again. This is an advanced security control, beyond what CIP-010 envisions, where real time checks are performed to ensure a cyber asset is compliant with security policy. The way the CIP standards are currently written, however, could preclude such advanced controls since this Remediation VLAN must be either part of an ESP or a separate ESP in order to host BCAs per CIP-005-5 R1. Requirements such as those in CIP-005 and CIP-010 need to be modified to allow for these more advanced features and controls.

Multi-Site Data Center Extensions (Super ESP)

There are technology solutions now that support very high levels of resiliency, so much so that virtual machines can be seamlessly moved from physical infrastructure at one data center across great distances to physical infrastructure at another data center. For example, control center functions could move easily and seamlessly from a primary control center to a backup control center across town or across the state. For this to work, an entity would use tunneling protocols that make the two data center networks appear as one local network ("layer 2 adjacency"). You've "stretched" a LAN across a WAN. The issue with CIP is that it assumes a LAN at each site with a defined ESP and access control at a point on that ESP at each site, with all the WAN communications equipment in between these ESPs exempted from scope. In

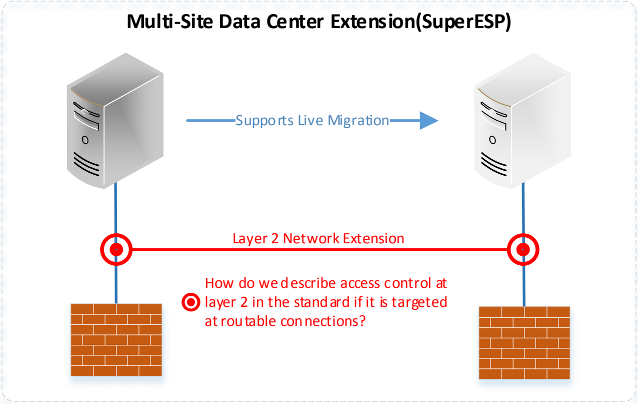


Figure 11

this situation, however, we have a single “local network” stretched between different sites creating at one level a “Super ESP”. Complicating the issue is that underneath this logical network extension, the data may actually ride in encrypted tunnels created at a routable protocol layer. At that layer, firewalls on an ESP can’t really provide any security, but that is prescriptively where the CIP standards say it must be done.

Chapter 3: Future Concept Example

Previously the proposed solution to address these issues with virtualization was a full embrace of the cyber system concept (retiring device level terms like Cyber Asset and BES Cyber Asset) and writing the technical requirements (e.g. CIP-005, CIP-007, CIP-010) at a more objective level. However, through industry feedback several important issues came to light:

- Eliminating the BES Cyber Asset definition and moving to the BES Cyber System as the sole foundational object with no further granularity would cause a complete overhaul and “do-over” of entities’ CIP-002 processes with insufficient benefit for the effort required.
- Requiring grouping systems by function exclusively conflicts with a number of different ways the industry has used the systems grouping flexibility; for example to group all Cyber Assets of a like operating system for patching purposes.
- Stating security objectives in requirements must be at a level where they are clearly measurable.

With these issues in mind, the future concept is to leave the foundational definitions largely unmodified. A “Cyber Asset” would remain as-is and be inclusive of the hardware as it is today. However, including the hardware for virtual cyber assets does not work, even though it needs to be protected the same as a discrete physical cyber asset. To resolve this the SDT will create a separate definition to capture virtual cyber assets so that they can be added to the applicability of the appropriate requirements. The hardware that provides compute, network, and storage resources would become its own new term to capture shared infrastructure and allow requirements to be written for risks unique to that environment. BES Cyber Systems would remain as-is and allow for all the various ways entities have used that concept to date.

The direction remains to establish objective level requirements but these need to be written at the appropriate level. For example, if CIP-005 R1 were written as “Mitigate the risk of unauthorized network access”, it is certainly an objective but is too high level to be measurable. No one would be able to state when, or to what degree this objective had been accomplished. If CIP-005 R1 were written as “Only allow known valid layer 3 IP addresses into or out of the network and implement this only at a Cyber Asset interface located only at the network edge”, it would be a prescribed topology and a prescriptive “how.” This should be avoided as it precludes much of the newer technologies presented in this paper. The latter is essentially the CIP-005 R1 of today and is one of the primary requirements that needs to change to remove this prescriptive topology and “how’s”.

An example of an alternative objective requirement that clearly describes a measurable “what” but avoids prescriptive “how’s” for CIP-005 R1 could conceptually be:

> *Deny all access to and from the networks on which high and medium impact BES Cyber Systems and their associated PCAs are connected and only allow network communication that has documented access permissions including the reason for granting access.*

This is a much clearer objective to accomplish but it avoids telling the entity how or where they must implement it or how their network must be architected. As for backward compatibility, an entity could still define an ESP with designated EAPs and provide firewall configurations as they do today. However, an entity using the advanced virtualization techniques from earlier in this paper, or future techniques to control network access that have not yet been contemplated can still show they meet this same objective.

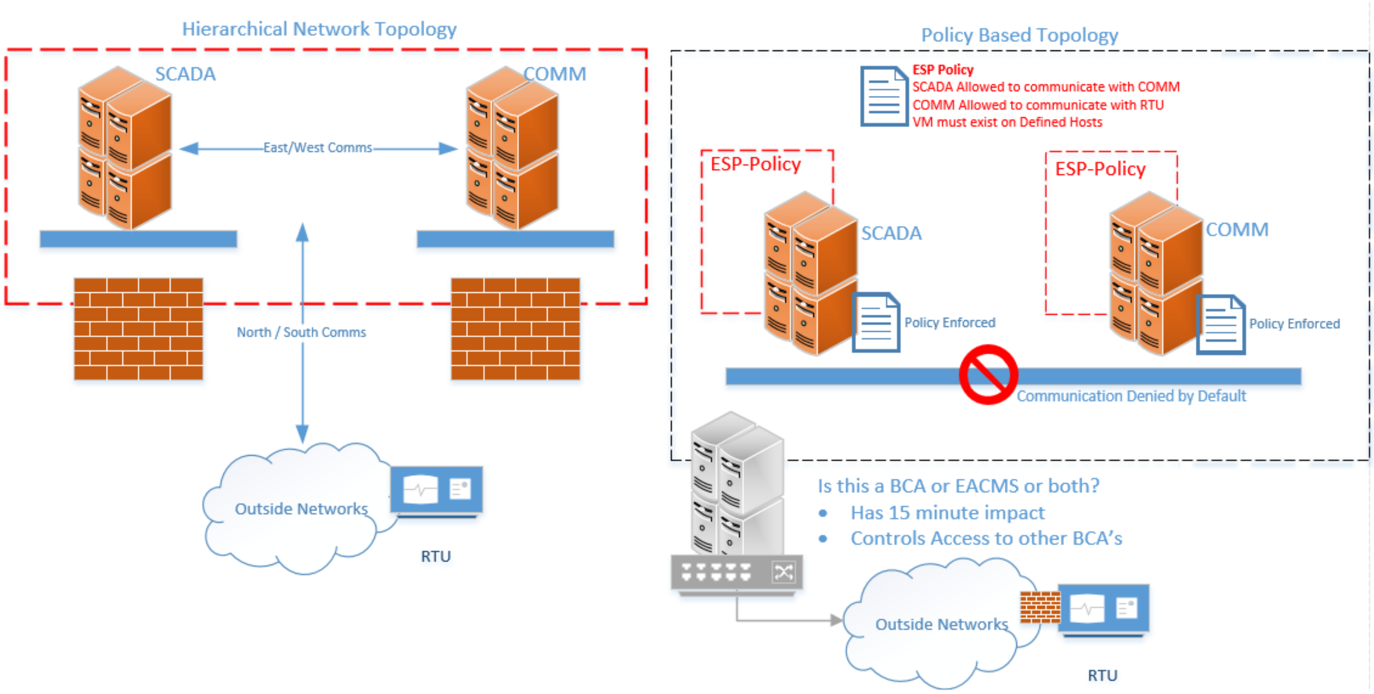


Figure 12

As shown in Figure 12, the current state ESP/EAP model on the left continues to be a valid architecture and topology with which to meet the objective. It is prescribed under the current requirements, but is not the ONLY way to accomplish the objective. On the right is a policy-based model in a fully virtualized system which can also accomplish the same objective once it is no longer prohibited by the requirement language. It has no distinct EAP; no distinct 'point' or 'interface' where the access controls are implemented. This is because the access policy is implemented throughout the infrastructure and the controls move with the virtual workloads. Access control is applied at a deeper level, closer to the functions that require protection and the policy allows no communication to occur that isn't explicitly allowed. The objective stated in the requirement can be met in either scenario.

For the asset classification, nothing changes for the architecture on the left. For the virtualized architecture on the right, the concept is to clarify that the systems in orange are virtual cyber assets, but without including the hardware. They exist as a virtual entity and need much of the same protection as a physical cyber asset. The systems depicted in grey are the Shared Infrastructure, a new asset class that hosts virtual cyber assets. Having these additional asset classes would allow the CIP standards to require protection appropriate to each class, whether a discrete physical system, a virtual cyber asset, or shared infrastructure hosting many virtual BES Cyber Systems.

Chapter 4: Conclusion

This paper has stepped through the benefits of virtualization in terms of increased reliability and resiliency for BES Cyber Systems. It also discusses how virtualization provides newer techniques for securing access to those systems, such as distributed firewalls and zero trust models. It has highlighted some of the issues created by several of these concepts and the required topologies contained within today's CIP requirements. Many of these issues revolve around the proper classification of cyber assets in virtualized environments and having asset classes whereby requirements can be properly scoped. Several other issues revolve around the prescriptive "how" of today's CIP-005 ESP/EAP model, the CIP-010 data requirements in a virtual storage world, or how CIP-011's requirements need minor changes to allow for technologies such as remediation VLAN's.

The CIP standards require some changes to:

- Address risks unique to virtualized environments such as the sharing of hardware resources and management plane access.
- Provide clarity around how to identify and categorize the various types of cyber assets in a virtualized infrastructure and scope requirements appropriately.
- Allow entities to fully implement newer security techniques in these environments that can provide higher levels of access control that are easier to manage, and don't require purchasing extra hardware to show compliance with prescribed topologies.

Many of these issues can be addressed as shown in the CIP-005 R1 example concept, where the prescriptive 'how' has been removed and replaced with a clearly stated security objective – one that fully allows for current state but also allows these newer techniques. Developing technology-agnostic security objectives can not only solve the issues presented by today's virtualization technologies, but also help address future issues brought about by technologies that aren't even contemplated today.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit E

Technical Rationale

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit E-1

CIP-002-7

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — BES Cyber System Categorization

Technical Rationale and Justification for Reliability Standard CIP-002-7

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-002-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-002-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-002-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a SDT. The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Attachment 1 – Impact Rating Criteria

Change Rationale:

In the medium impact rating criterion 2.1 referencing shared BCS for commissioned generation, the SDT has proposed a change to incorporate an earlier approved Request For Interpretation (RFI). The RFI was submitted seeking clarification of Criterion 2.1 of Attachment 1 regarding the use of the phrase "shared BES Cyber Systems." The resulting approved interpretation was introduced as Appendix 1 in CIP-002-5.1a.

The SDT incorporated the interpretation into CIP-002-7 Attachment 1 criterion 2.1 by modifying it to reference "each discrete shared BCS" and removed the RFI appendix from the standard.

Former Background Section from Reliability Standard CIP-002-5.1a

The **Background** section has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

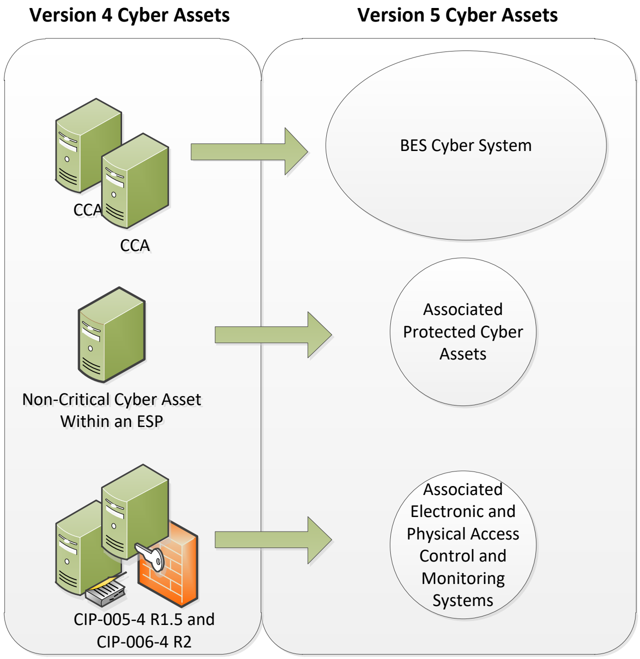
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their Bulk Electric System (BES) Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the BES. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily

to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term “BES Cyber System” is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity’s responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than “Real-time,” BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4, and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS")

Examples include Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")

Examples include authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA")

Examples may include, to the extent they are within the ESP file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

Technical Rationale for Reliability Standard CIP-002-5.1a

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from the CIP-002-5.1a standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1a

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints

- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
    - Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)

        - Special Protection Systems or Remedial Action Schemes
    - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
        - Under and Over Frequency relay protection (includes automatic load shedding)
    - Sensors, relays & breakers (DP)
        - Under and Over Voltage relay protection (includes automatic load shedding)
    - Sensors, relays & breakers (DP)
        - Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions, and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
    - Field data sources (real time tie flows, frequency sources, time error, etc.) (TO, TOP)
    - Software used to perform calculation (BA)
- Demand Response
    - Ability to identify load change need (BA)
    - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
    - Ability to identify load change need (BA)
    - Ability to implement load changes (TOP, DP)
- Non-spinning reserve (contingency reserve)
    - Know generation status, capability, ramp rate, start time (GO, BA)
    - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
    - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
    - Software to calculate unit adjustments (BA)
    - Transmit adjustments to individual units (GOP)
    - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
    - Frequency source, schedule (BA)
    - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
    - Sensors, stator control system, feedback (GO)
- Capacitive resources
    - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
    - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
    - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
    - SCADA (TOP, GOP)
    - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions, and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
    - Through black start units (TOP, GOP)
    - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive, or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term “Facilities”, there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports

the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.

- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1’s medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is “to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance.” In particular, it requires that “as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency.” The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.

In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities’ qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a “long term” reliability planning, i.e. that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as “Reliability Must Run,” and this designation is distinct from those generation Facilities designated as “must run” for market stabilization purposes. Because the use of the term “must run” creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.
- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.
- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e., fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.
- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.
- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:
  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

- 230 kV –> 700 MVA
- 345 kV –> 1,300 MVA
- 500 kV –> 2,000 MVA
- 765 kV –> 3,000 MVA

In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

- For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would consider the connections in and out of each station or substation location.
- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.
- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIRs are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.
- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.
- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise, or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.
- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

  In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.
- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that “control” 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC’s Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

  Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

  BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator’s restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator’s restoration plan. The glossary term Blackstart Capability Plan has been retired.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to “provide the entities identified in

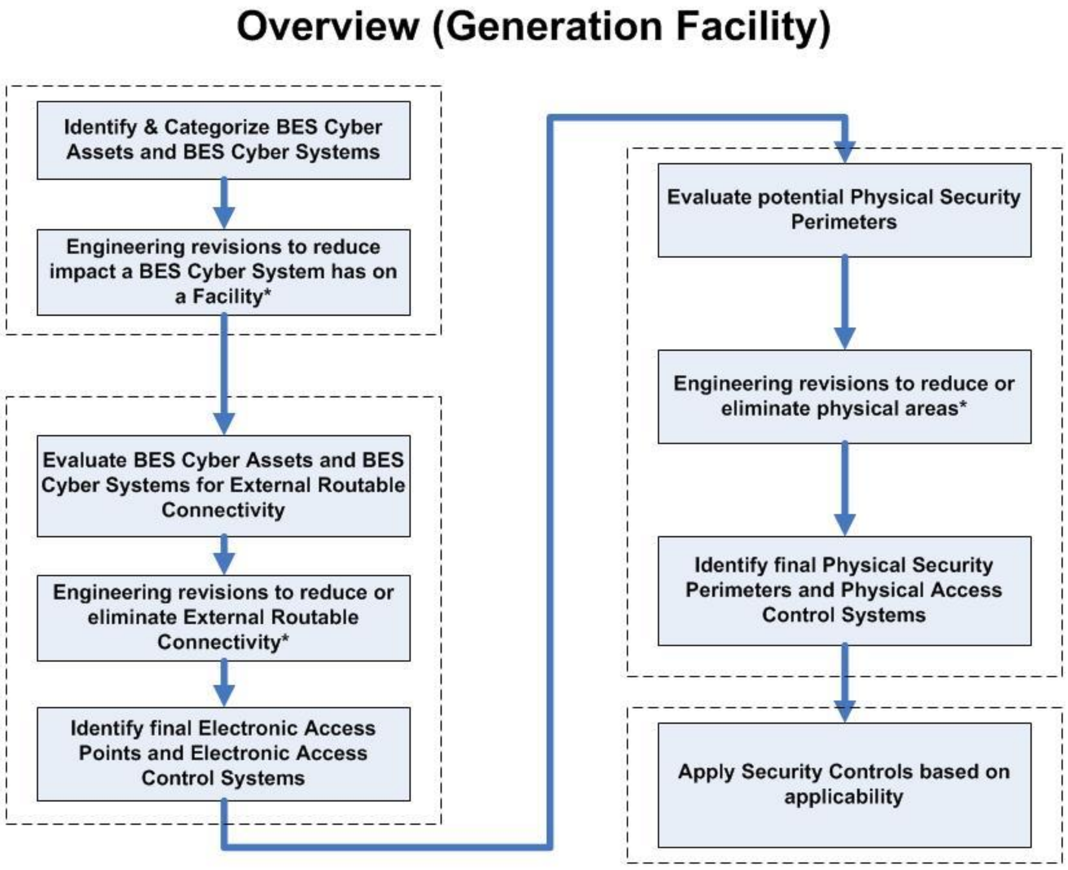
its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan.”

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator’s restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator’s Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the BES. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Appendix 1

Requirement Number and Text of Requirement

<u>CIP-002-5.1, Requirement R1</u>

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

- i. Control Centers and backup Control Centers;
- ii. Transmission stations and substations;
- iii. Generation resources;
- iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

<u>Attachment 1, Criterion 2.1</u>

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions

Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase “shared BES Cyber Systems.”

The Interpretation Drafting Team identified the following questions in the RFI:

1. Whether the phrase “shared BES Cyber Systems” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?
2. Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?
3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

Responses

Question 1: Whether the phrase “shared BES Cyber Systems,” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states “Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…” Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states “*Each BES Cyber System*…associated with any of the following [criteria].” (emphasis added)

Additionally, the Background section of CIP-002-5.1 states that “[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System.” The Background section also provides:

> The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Question 2: Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term “shared” is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.” For criterion 2.2: “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit E-2

CIP-003-10

RELIABILITY | RESILIENCE | SECURITY

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-10

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-003-10

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-10. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-10 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document stated, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-10 to shorten applicability statements within the body of CIP standards with "BCS" as the defined acronym for "BES Cyber System".

Requirement R2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-10 to align security management control requirements with the virtualization changes.

To ensure SCI supporting low impact BCS is afforded equal security controls as the BCS, the SDT added "SCI that supports a low impact BCS". Where shared infrastructure is serving only low impact BCS it would not meet the 2nd component of the first bullet in the SCI definition and therefore would not qualify as SCI; However, in this scenario the shared infrastructure becomes a component of the low impact BCS and would remain subject to the Requirements within R2.

Attachment 1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-10 to shorten applicability statements within the body of CIP standards with "BCS" as the defined acronym for "BES Cyber System".

To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a system(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term system(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Attachment 1 Section 2

Rationale

To ensure virtual infrastructure providing electronic access controls for the low impact BCS is afforded equal physical security controls as the physical Cyber Assets that provide electronic access controls for the low impact BCS, the SDT modified this section to include the Virtual Cyber Asset (VCA) where only Cyber Assets had previously been listed.

Attachment 1 Section 3 Part 3.1

Rationale

Part 3.1(i)

To ensure an asset containing a low impact BCS or an SCI supporting a low impact BCS is afforded equal electronic access controls as the low impact BCS, the SDT added "SCI that supports a low impact BCS and a Cyber System(s) outside the asset containing the low impact BES Cyber System (BCS); or the SCI that supports a low impact BCS"".

To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a Cyber System(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term Cyber System(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Part 3.1(ii) To ensure only necessary inbound and outbound electronic access is permitted for SCI that supports a low impact BCS just as is required for access control to the low impact BCS, the SDT adjusted the language to include communications that are between SCI that supports any part of a low impact BCS and a system(s) outside the asset(s) containing the SCI that supports any part of a low impact BCS.

Part 3.1 (iii) The SDT replaced the undefined 'intelligent electronic devices' with the defined term 'Protection Systems'.

Attachment 1 Section 3 Part 3.2

Rationale

To ensure SCI supporting low impact BCS are afforded equal electronic access controls for Dial-up Connectivity, the SDT added "or SCI that supports a low impact BCS". To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the ‘per Cyber Asset capability’ was changed to ‘per system capability’.

Attachment 1 Section 5 Part 5.2

Rationale

The final bullet of Attachment 1 Section 5 Part 5.2.1 was preceded with the language “Review of” to make the requirement for other methods parallel to the five options listed above it.

Attachment 1 Section 5 Part 5.3

Rationale

To enable for virtualization technologies and capabilities the SDT added, “or VCA” in Attachment 1 Section 5 Parts 5.3.1.

To ensure SCI supporting a low impact BCS are afforded equal protections from malicious code when using Removable Media, the SDT added “SCI that supports a low impact BCS” to the low impact BCS in Attachment 1 Section 5 Parts 5.3.1 & 5.3.2.

Attachment 2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-10 to shorten applicability statements within the body of CIP standards with “BCS” as the defined acronym for “BES Cyber System”. Additional changes were to align the Attachment 2 Measures with the modifications to the Attachment 1 requirement language.

Technical Rationale for Reliability Standard CIP-003-9

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-003-9 standard to preserve any historical references. No modifications have been made.

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-9. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-9 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2020-03 – Supply Chain Low Impact Revisions Standards Drafting Team (SDT) intent in drafting changes to the requirement.

Background

In its final report[1] accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact Bulk Electric System (BES) Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through Member Representatives Committee (MRC) Policy Input.

After considering policy input, the NERC Board adopted a resolution[2] to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Foreword Regarding Section 3 and Section 6

When developing the standards language for this SAR, the SDT considered many variables and inputs to draft clear, concise, and meaningful requirements. The SDT considered the scope and variety of entity sizes, functions, organizations, systems and configurations, entity business processes, remote access, local electronic access, remote access architectures and technologies, and data path and communications protocols. The SDT discussed systems used for electronic access, remote vs local electronic access, vendor access accounts and privileges, and optimal time frames for establishing, identifying, determining, and disabling or terminating vendor electronic access.

---

[1] Supply Chain Risk Assessment Report (nerc.com)

[2] FINAL_Minutes_BOT_Open_Meeting_February_2020.pdf (nerc.com)

The SDT reviewed industry comments and draft language suggestions, existing standards, and discussed and deliberated the options and their potential impacts and interpretative values to industry. The SDT recognized that some entities may use the same process, system and/or technology (for vendor electronic access) that is used by entity personnel, or cases where entities use separate processes, systems, or technologies to manage vendor electronic access. The SDT also discussed systems and Cyber Assets owned by vendors but authorized for use on entity networks, vs systems and Cyber Assets owned by entities but used by vendors for electronic remote access. Because of the variety, the SDT focused on allowing entities to identify their particular risks related to remote vendor electronic access and define processes and plans to define and implement security controls to address those risks.

In reviewing the industry comments, the SDT identified, discussed and considered additional terms for clarification, and came to the following conclusions:

1. Electronic remote access: considered remote access as definition and/or remote access vs electronic remote access - as well as onsite vs off-premises remote access. The use of electronic remote access clarifies the remote access using a method (non-physical) which matches existing electronic remote access in other CIP standards.
2. Interactive Remote Access: avoided the existing NERC Glossary of Terms definition in order to prevent applying high and medium impact requirements upon low impact assets and systems.
3. Active: avoided using this term due to potential unintended consequences. The use of “active” may add further requirements upon entities to define, track and document when “active” occurs vs when it does not.
4. Read-only: avoided using this term due to potential unintended consequences. The use of “read-only” may add further requirements upon entities to define and document systems and processes which are read-only from read-write, and where and when read-only access occurs.
5. Vendor: CIP-013 Supplemental Material[3] addresses the term vendor in context with applicable high and medium BES Cyber Systems. The SDT avoided defining the term vendor specifically within the low impact standards to avoid conflicts for entities with high, medium, and low impact systems.

The language developed gives entities the flexibility to define processes to identify and manage vendor electronic remote access for their specific policies, processes, systems, configurations, organizations, operations, and BES Facilities. The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access.

The SDT agreed to retain Section 3 of CIP-003-9 Requirement R2, Attachment 1 and established Section 6 to specifically address low impact vendor electronic remote access, as well as malicious inbound and outbound data communications which may be sourced from or transmitted to vendors. Based on the SAR, the SDT did not include dial-up from Section 3.2.

The language requires an entity to develop and implement a process or processes for identifying vendor electronic remote access, having a method or methods for disabling vendor electronic remote access, as well as methods to detect known or suspicious vendor inbound and outbound malicious communications.

Entities may choose to define systems, applications and/or configurations used by vendors, accounts and privileges, network data communication paths or physical processes for establishing and disabling vendor electronic remote communications. Section 6 provides the flexibility to meet many types of vendor electronic remote access configurations while managing vendor electronic remote access risks.

---

[3] CIP-013 Technical Rationale

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine vendor electronic remote access is initiated; and (3) disable vendor electronic remote access when necessary.

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately 66% have external connectivity which often results in the allowance of vendor electronic remote access. As our grid has grown more complex, the use of external parties to support and maintain low impact BES Cyber Systems, equipment and facilities is expected. However, the prevalence of external connectivity across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this vulnerability, the originating FERC Order[4], and the resulting NERC Board resolution[5], the proposed Attachment 1 Section 6, as it relates to the existing Requirement R2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and vendor electronic remote access.

Attachment 1 Section 6 Part 6.1 – Determining vendor electronic remote access

The objective of Attachment 1 Section 6.1 is for entities to determine vendor electronic remote access to their low impact BES Asset(s) and/or BES Cyber Systems. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access. The obligation in Section 6.1 requires that entities have one or more methods for determining vendor electronic remote access.

Attachment 1 Section 6 Part 6.2 – Disabling vendor electronic remote access

The objective of Attachment 1 Section 6.2 is for entities to have the ability to disable vendor electronic remote access for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing low impact BES Cyber Systems. The obligation in Section 6.2 requires that entities have a method to disable vendor electronic remote access, which in turn supports the security objective to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications from vendors, such that the entity may respond to and remediate any resulting adverse impacts.

This sub section is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with assets containing low impact BES Cyber Systems.

---

[4] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[5] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)

Current obligations in CIP-003-8 Requirement R2 that govern direct electronic communications with low impact BES Cyber Systems are not as robust as those in CIP-005-6 that govern high impact medium impact BES Cyber Systems. Security controls such as use of Intermediate Systems and multi-factor authentication provide additional security protection from malicious communication and overall access controls for high and medium impact BES Cyber Systems. In addition to Intermediate Systems and multi-factor authentication, high and medium impact BES Cyber Systems at Control Centers have requirements to detect malicious communications at the Electronic Access Points of those systems. These security measures are not required at low impact BES Cyber Systems.

In keeping with the NERC stated risk-based model, there may be a scenario where a vendor directly communicates with a low impact BES Cyber System. In the event that this connection may be compromised, the inclusion of security requirements to detect malicious communications under CIP-003-9 Attachment 1 Section 6 would provide entities visibility and opportunity in detecting and mitigating risks posed by vendor communications.

Former Background from Reliability Standard CIP-003-8

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background
Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Technical Rationale for Reliability Standard CIP-003-8

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-003-8 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media

- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only “necessary” inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for “necessary” inbound and outbound electronic access controls may be documented within the Responsible Entity’s cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

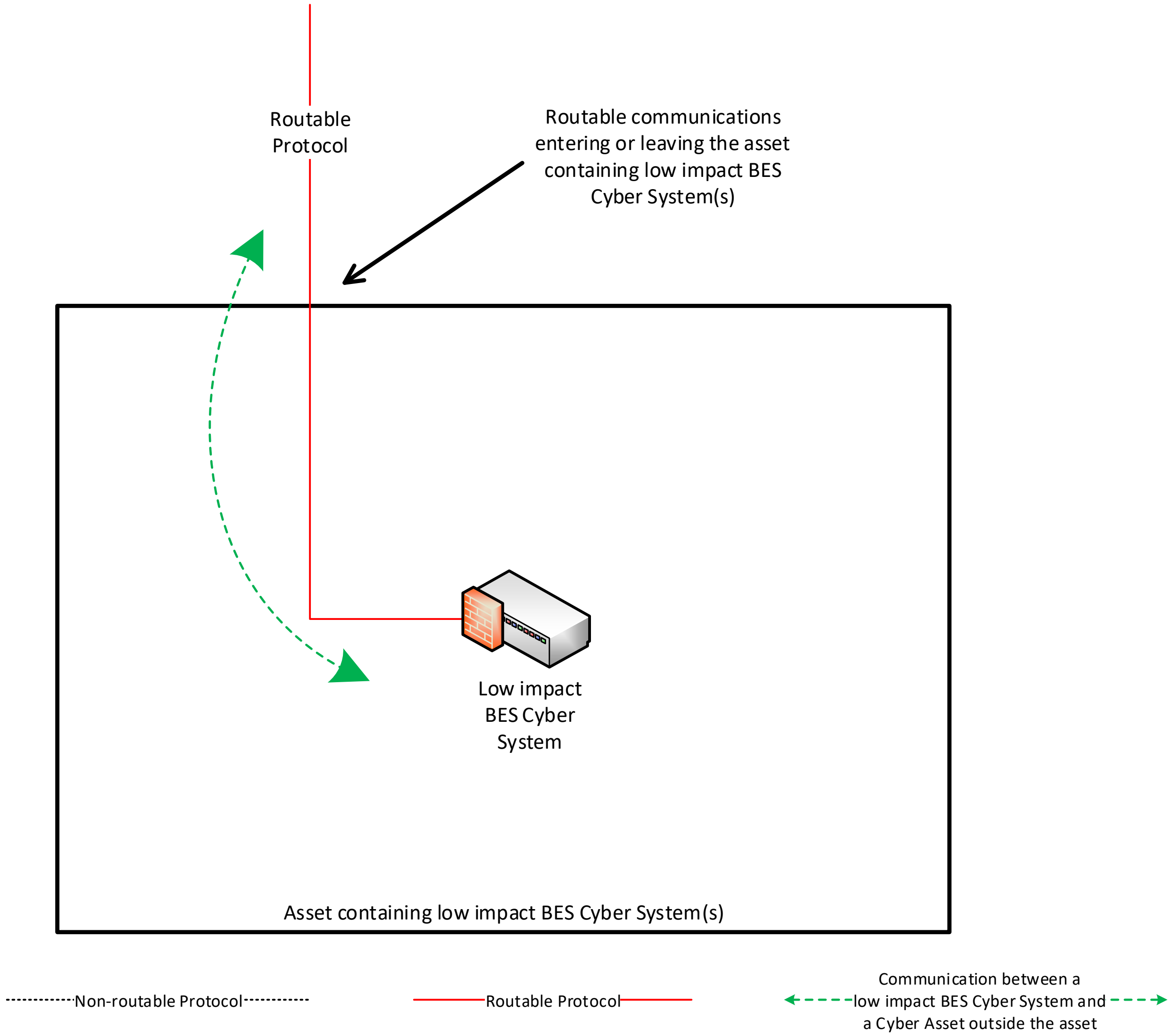
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

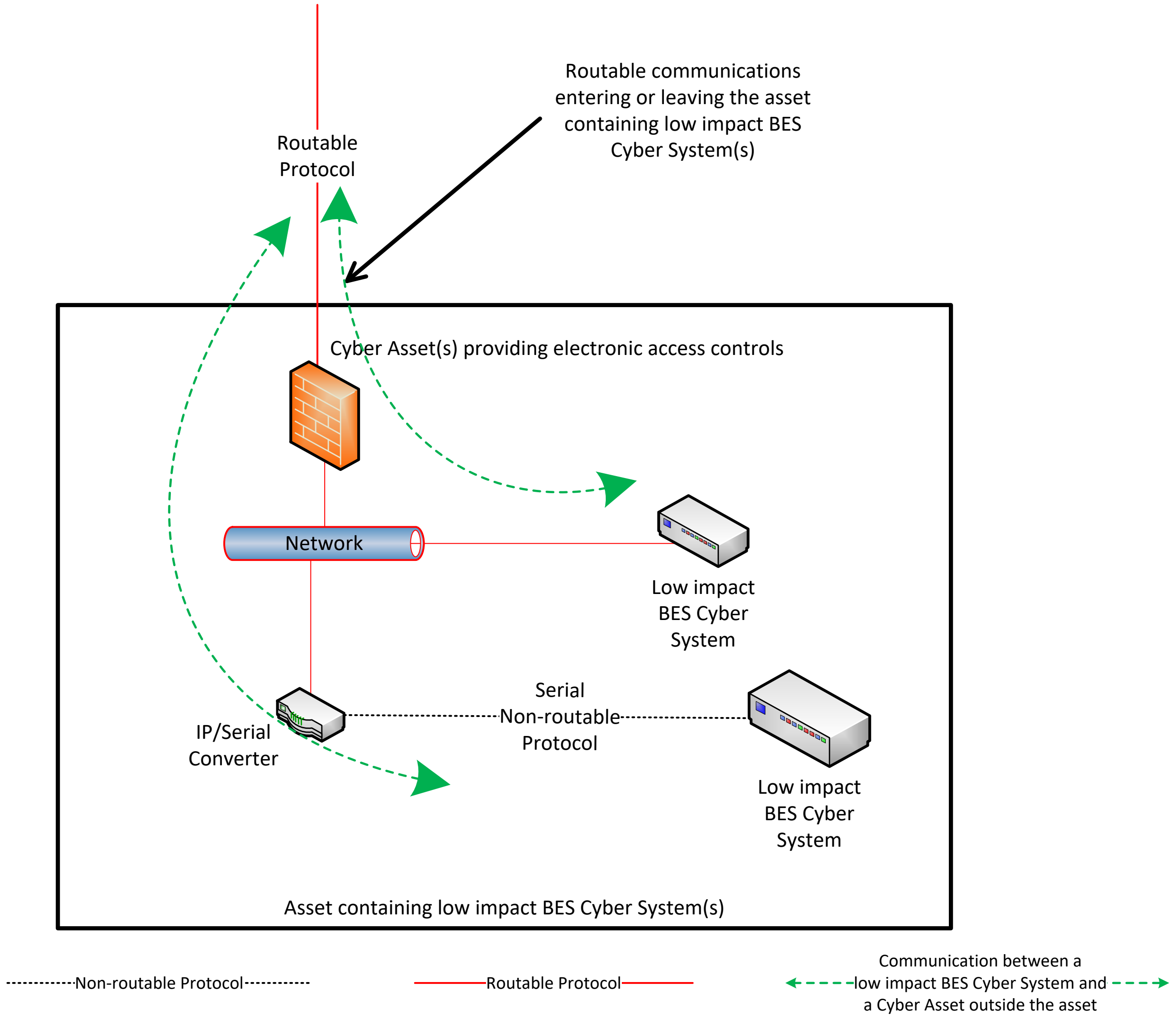
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

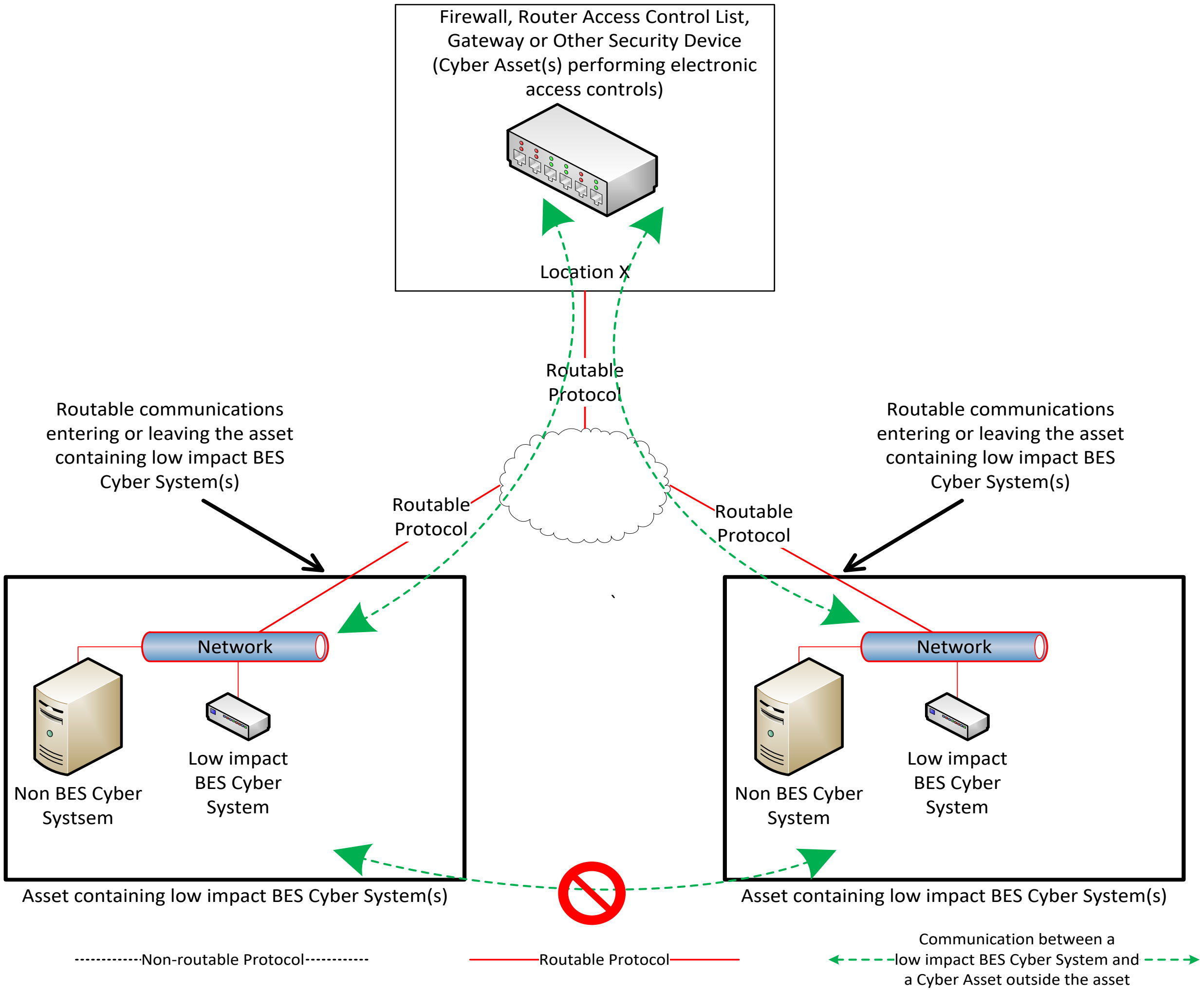
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

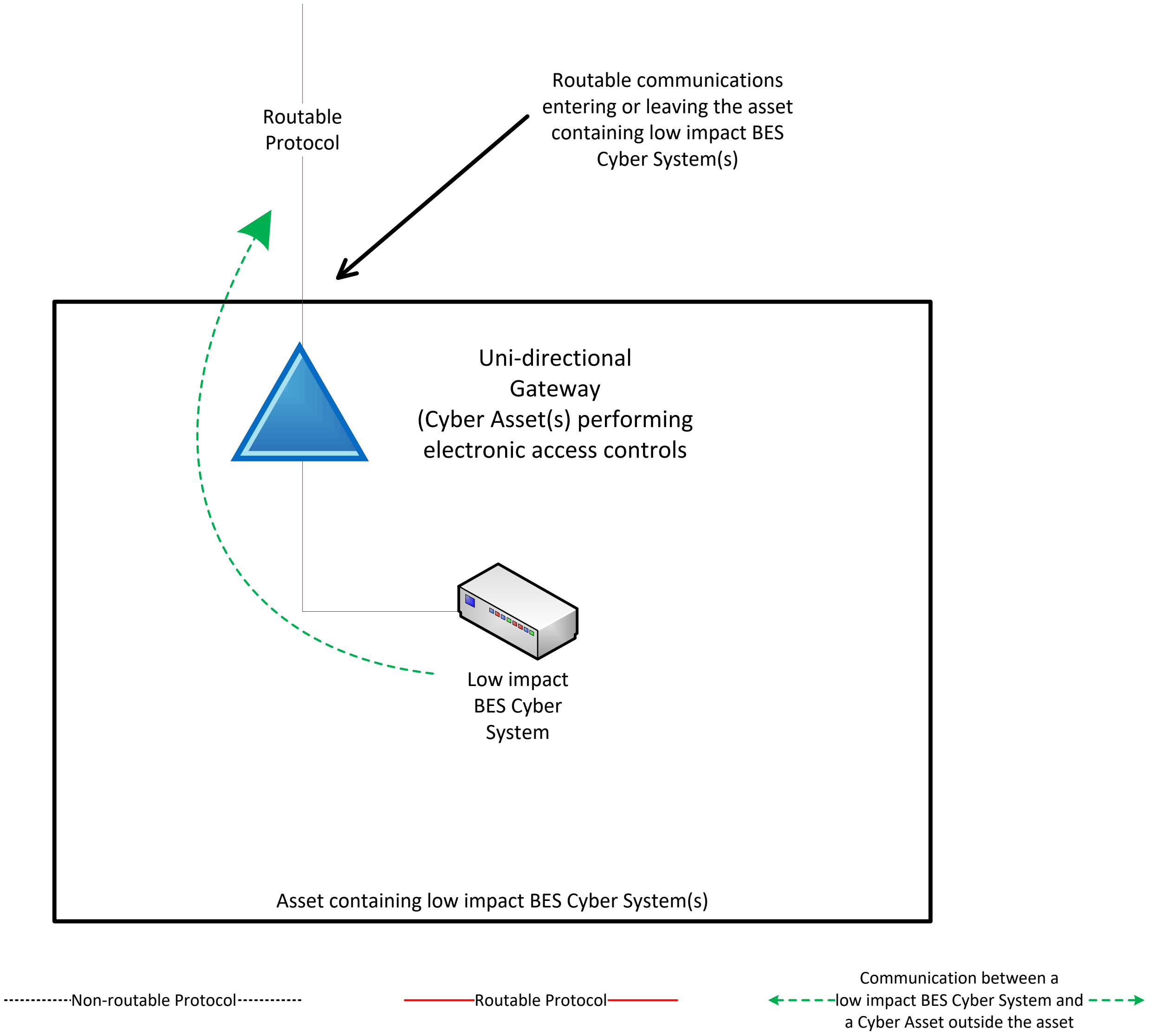
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

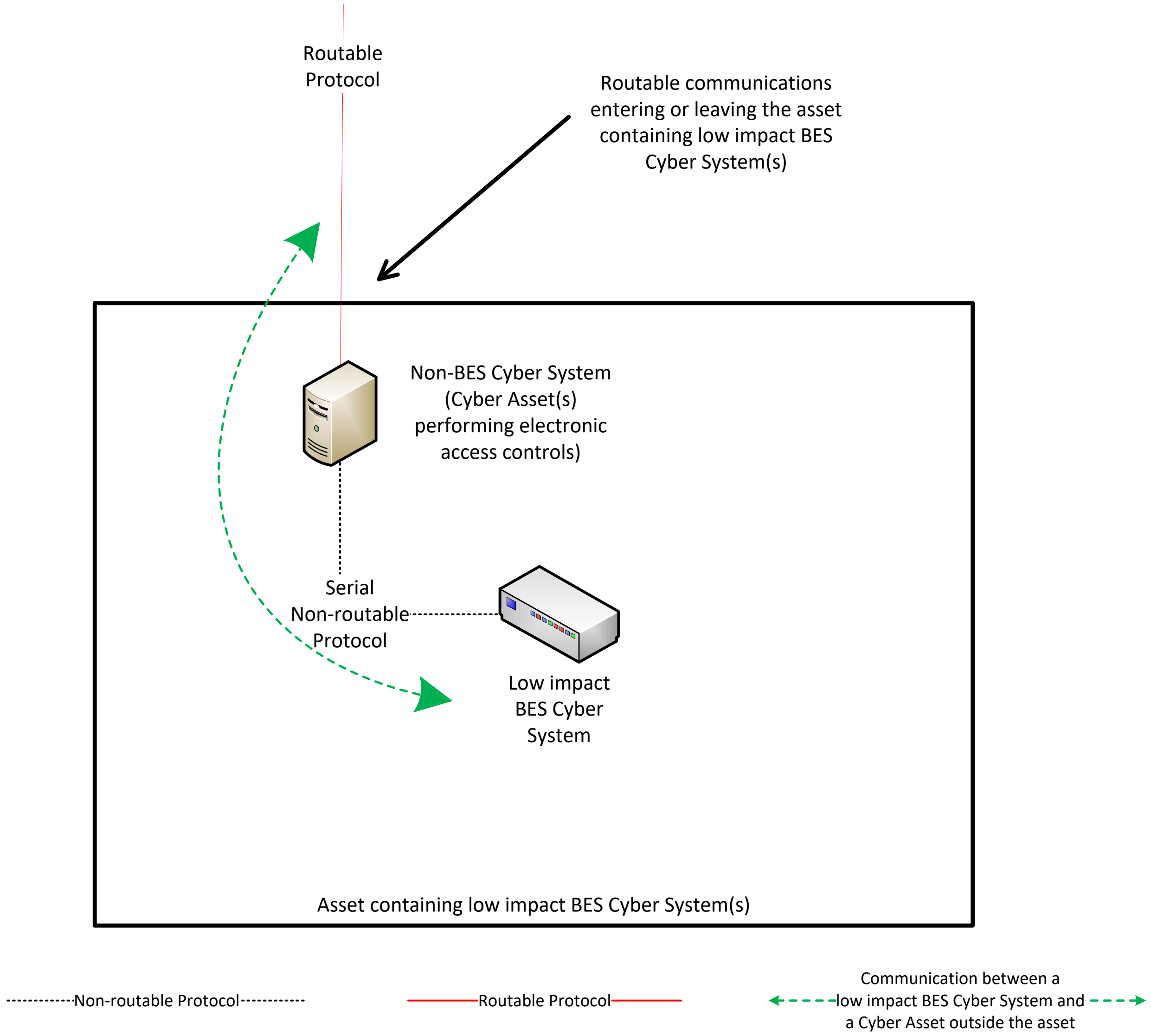
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a “one-way” (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

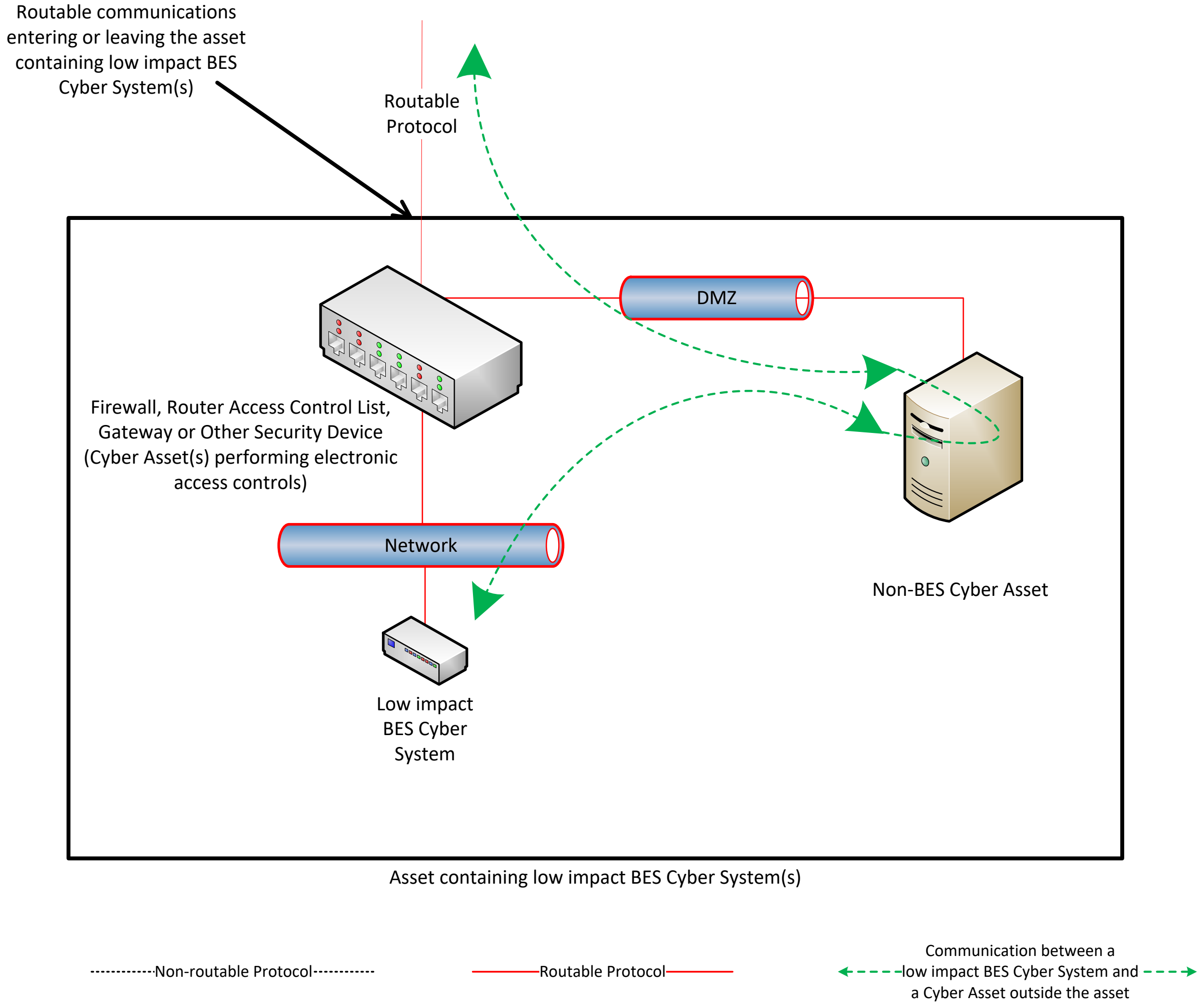
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

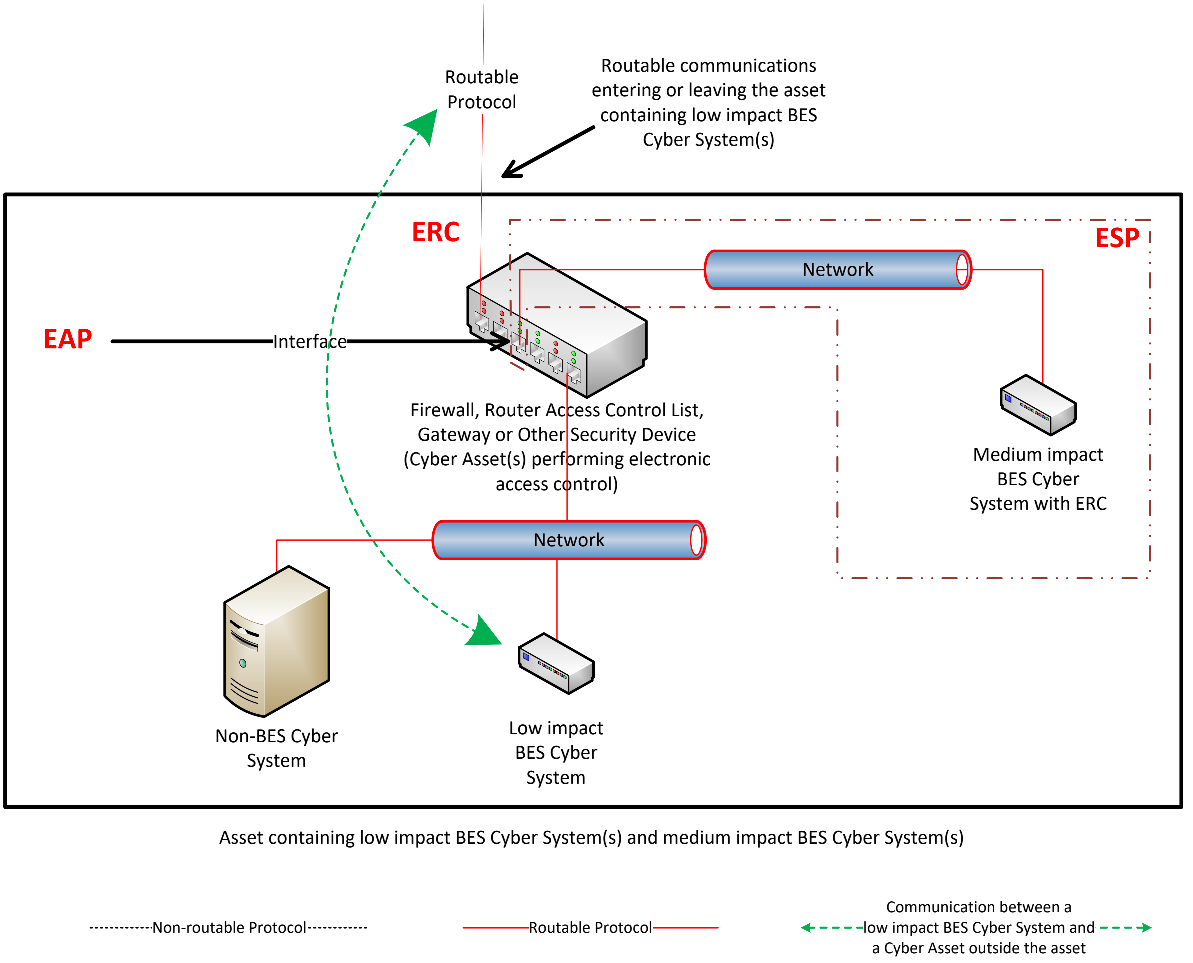
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.



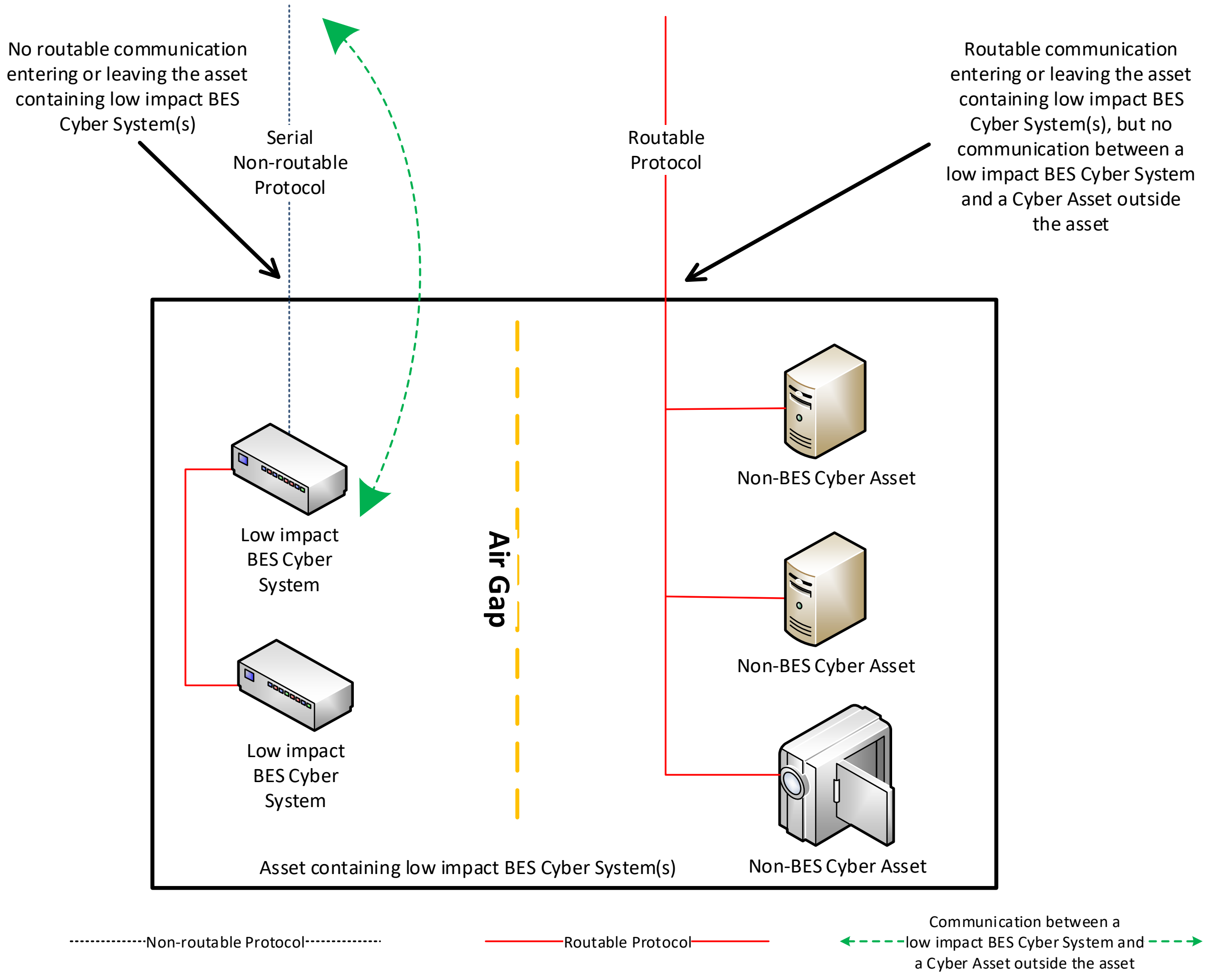
Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).

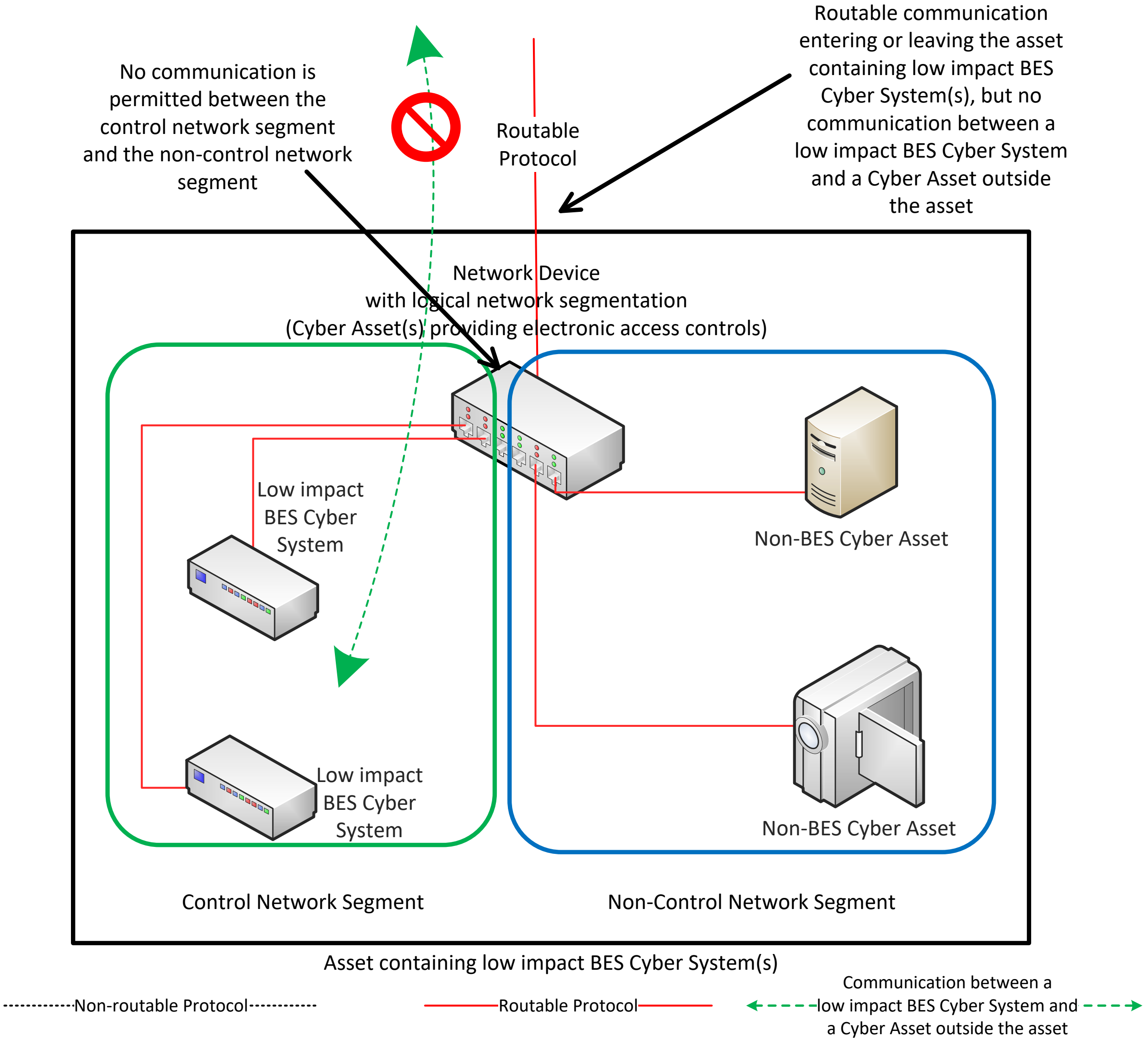
Section 1.



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.

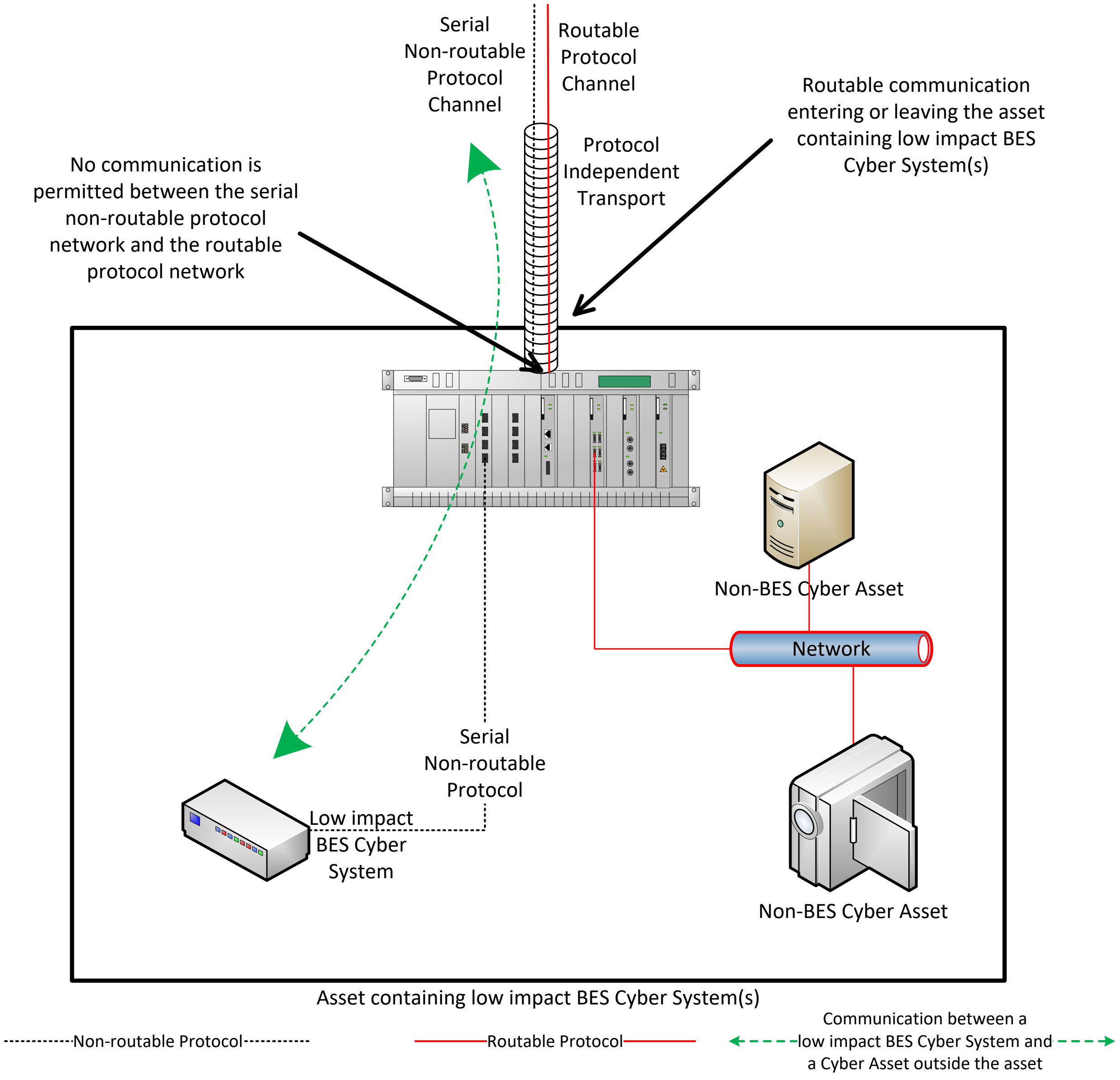

No communication is permitted between the control network segment and the non-control network segment

Routable communication entering or leaving the asset containing low impact BES Cyber System(s), but no communication between a low impact BES Cyber System and a Cyber Asset outside the asset

Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity’s response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, “A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.” The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[6] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity

---

[6] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2.1: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Section 5.2.2: The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity’s BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management’s commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):
Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):
Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for “clear lines of authority and ownership for security matters.” With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit E-3

CIP-004-8

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-8

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-004-8

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-004-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the issues identified by the V5TAG was virtualization. The V5TAG Transfer document states, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." Document for reference when reading the technical rationale that follows.

Requirement R1-R6

General Considerations

For Requirements R2 through R6, the Project 2016-02 SDT added a new type of 'Applicable System' called '**Medium impact BCS with IRA**'. As the SDT is addressing IRA to a non-routable BCA/BCS through scenarios such as IP-to-serial conversion, IRA is no longer dependent on ERC and "associated ESPs". Therefore, CIP-004 requirements for provisioning and deprovisioning IRA for personnel can no longer be limited to only medium impact BCS with ERC.

However, several of the Requirement Parts cover both physical and electronic access and the "with ERC" has been used as a scoping filter so that, for example, you don't have to deprovision physical access within 24 hours at a remote site that has no ERC and changes for physical security may require a site visit. To account for this situation, several of the Requirement Parts now include a "(except for Medium impact BCS without ERC)" exclusion on the physical access portions of the language.

Note that by adding this to Requirement 2, Part 2.1 it does not mean that all personnel who would ONLY need IRA (i.e., vendors with occasional remote access needs) would need training on all content listed. R2 states the training program is "appropriate to individual roles, functions, or responsibilities".

The Project 2016-02 SDT also made conforming changes to Reliability Standard CIP-004-8 to align personnel and training requirements with the virtualization changes.

To enable CIP-004-8 for virtualization, the SDT added "Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part" within the Applicable Systems column of each of the Parts for Requirement R1 – Requirement R6.

Additionally, where the term BES Cyber System (BCS) was used in the requirement language, it is replaced with "Applicable Systems" to align the requirement language of each Requirement Part with the updated applicability for each Requirement Part.

Requirement R3 Part 3.5

Summary of Changes:

A CIP Exceptional Circumstance was added as an exception to "Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 through 3.4 within the last seven years" such that individuals granted authorized electronic access and authorized unescorted physical access have undergone the personnel risk assessment processes.

Change Rationale:

The SDT determined Responsible Entities cannot require personnel risk assessments for first responders prior to granting them authorized unescorted physical access during certain conditions that qualify as CIP Exceptional Circumstances.

Former Background Section from Reliability Standard CIP-004-7

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

The following conventions are used in the “Applicable Systems” column as described. High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-004-7

General Considerations for Requirement R1

None

Rationale for Requirement R1

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table Requirement R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets (TCA) and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, TCA and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3

General Considerations for Requirement R3

None

Rationale for Requirement R3

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new personnel risk assessment (PRA). Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4

General Considerations for Requirement R4

None

Rationale for Requirement R4

Authorization for electronic and unescorted physical access must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5

General Considerations for Requirement R5

None

Rationale for Requirement R5

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5 Part 5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement R5 Part 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the Bulk Electric System. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Requirement R6

General Considerations for Requirement R6

None

Rationale for Requirement R6

Requirement R6 requires Responsible Entities to implement a BES Cyber System Information (BCSI) access management program to ensure that provisioned access to BCSI is authorized, verified, and promptly revoked. Authorization ensures only individuals who have a need are authorized for provisioned access to BCSI. Prompt revocation of terminated individuals’ ability to access BCSI helps prevent inappropriate disclosure or use of BCSI. Periodic verification ensures that what is currently provisioned is authorized and still required, and allows the Responsible Entity the opportunity to correct any errors in provisioning.

The change to "provisioned access" instead of "designated storage locations" enables the use of third-party solutions (e.g., cloud services) for BCSI. The concept of "designated storage locations" is too prescriptive and limiting for entities that want to implement file-level rights and permissions (i.e., policy based credentials or encryption keys that follow the file and the provisioned individual), which provide BCSI access controls regardless of storage location. The concept of provisioned access provides the needed flexibility for entities to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

According to Requirement R6, Part 6.1, the Responsible Entity must authorize individuals to be given provisioned access to BCSI. First, the Responsible Entity determines who needs the ability to obtain and use BCSI for performing legitimate work functions. Next, a person empowered by the Responsible Entity to do so authorizes—gives permission or approval for—those individuals to be given provisioned access to BCSI. Only then would the Responsible Entity provision access to BCSI as authorized.

Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI.

For BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet. For BCSI in electronic format, electronic access is provisioned to an electronic system or its contents, or to individual files. Provisioned physical access alone to a physical location housing hardware that contains electronic BCSI is not considered to be provisioned access to the electronic BCSI. Take, for instance, storing BCSI with a cloud service provider. In this case, the cloud service provider's personnel with physical access to the data center is not, by itself, considered provisioned access to the electronic BCSI stored on servers in that data center, as the personnel would also need to be provisioned electronic access to the servers or system. In scenarios like this, the Responsible Entity should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011-X. The subparts in Requirement R6, Part 6.1 were written to reinforce this concept and clarify access management requirements.

The periodic verification required by Requirement R6 Part 6.2 is to ensure that only authorized individuals have been provisioned access to BCSI and that what is provisioned is what each individual currently needs to perform work functions. For example, by performing the verification, the Responsible Entity might identify individuals who have changed jobs and no longer have a need for provisioned access to BCSI, and would therefore revoke provisioned access.

For Requirement R6 Part 6.3, removal of an individual's ability to use provisioned access to BCSI is considered to mean a process with the result that electronic access to electronic BCSI and physical access to physical BCSI is no longer possible from that point in time onwards using the means the individual had been given to obtain and use BCSI in those circumstances. Either what was specifically provisioned to give an individual access to BCSI (e.g., keys, local user or database accounts and associated privileges, etc.) is taken away, deleted, disabled, revoked, etc. (also known as “deprovisioning”), or some primary access is removed which prevents the individual from using the specifically provisioned means. Requirement R6 Part 6.3 acknowledges that where removing unescorted physical access and Interactive Remote Access, such as is required in Requirement R5 Part 5.1, prevents any further access to BCSI by the individual after termination, then this would constitute removal of an individual’s ability to use provisioned access to BCSI. Access can only be revoked or removed where access has been provisioned. The intent is not to have to retrieve individual pieces of BCSI (e.g., documents) that might be in someone’s possession (although you should if you can, but the individual cannot un-see what they have already seen).

Where no specific mechanisms are available or feasible for provisioning access to BCSI, these requirements are not applicable. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BCSI, such as when the individual is handed a piece of paper during a meeting or sees a whiteboard in a conference room. Likewise, these requirements are not applicable where provisioned electronic or physical access is not specifically intended to provide an individual the means to obtain and use BCSI. There will likely be no specific provisioning of access to BCSI on workstations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BCSI is only temporarily or incidentally located or stored there. Another example is the provisioning of access to a substation, the intent of which is to enable an individual to gain access to the substation to perform substation-related work tasks, not to access BCSI that may be located there. However, BCSI in these locations and situations still needs to be protected against unauthorized access per the Responsible Entity’s information protection program as required by CIP-011-X.

The change to “provisioned access” to BCSI is backwards compatible with the previous “designated storage locations” concept. Entities have likely designated only those storage locations to which access can be provisioned, rather than any location where BCSI might be found. Both concepts intend to exclude those locations where BCSI is temporarily stored, as explained in the previous paragraph. Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of information. The removal of the term “designated storage location” does not preclude an entity from defining storage locations for the entity’s access management program for authorization, verification, and revocation of access to BCSI.

Technical Rationale for Reliability Standard CIP-004-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

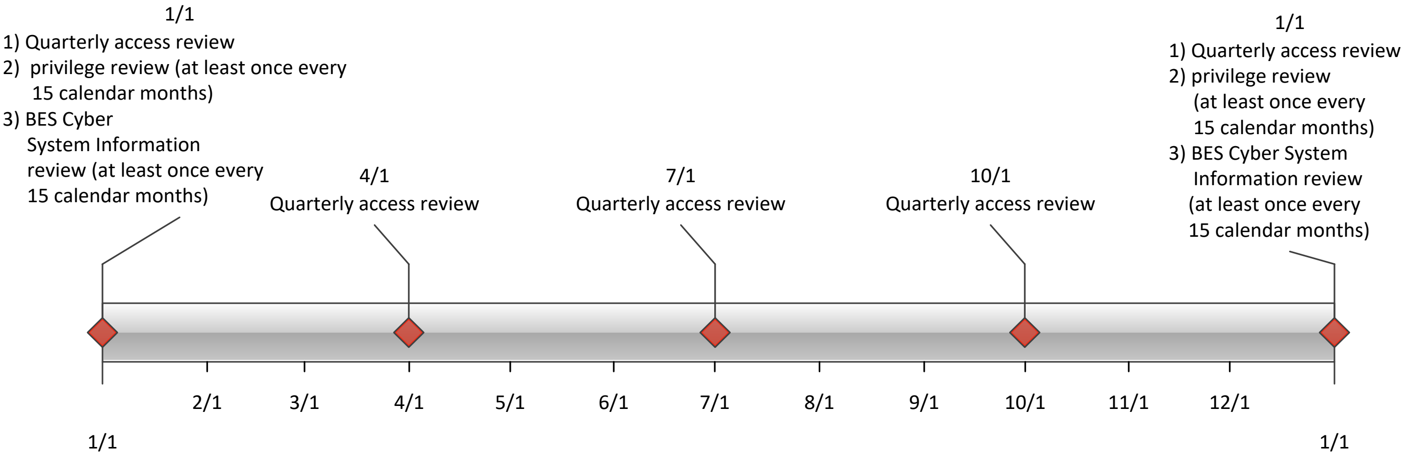
A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.



Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing “immediate” revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

Exhibit E-4

CIP-005-8

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security – Electronic Security Perimeter(s)

Technical Rationale and Justification for Reliability Standard CIP-005-8

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-005-8

Introduction

This document is the technical rationale and justification for Reliability Standard CIP-005. It includes the rationale for changes in the current proposed version (CIP-005-8) as well as previous versions of the standard. The intent of this document is to provide stakeholders and the ERO Enterprise with an understanding of the revisions and the technical concepts of the Reliability Standard as well as the rationale for such revisions, both the currently proposed and historical revisions from previous versions and SDTs.

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition Advisory Group (V5TAG), which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005-8 and the definitions of Cyber Asset and Electronic Access Point (EAP) that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

Summary

The Project 2016-02 Standard Drafting Team (SDT) proposal accommodates for increasing use of virtualization and other technology innovation. The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards, but also to better position the CIP standards to be applicable to additional future technological innovation while, to the extent possible, maintaining backwards compatibility.

CIP-005-8 remains a standard concerned with controlling communications to and from BES Cyber Systems (BCS) by establishing an Electronic Security Perimeter (ESP) with increased security controls for Interactive Remote Access (IRA) and vendor remote access. However, virtualization is enabling models for network security, such as "Zero Trust", that are not network perimeter based. Therefore, in CIP-005-8 the ESP focuses on being a security model rather than a network topology-based perimeter as the only option. Securing the communications to and from BCS is the security objective, but the standard no longer prescribes "where", as in where on a network, the controls must be implemented. Innovations such as Zero Trust models are moving access control from network borders to a session level orientation and eliminating the implicit trust within a local network. Network perimeter-based ESP and EAP implementations remain a valid option and are one method for allowing only necessary communications to the Cyber Systems within the ESP.

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in “CIP Definitions and Exemptions Technical Rationale” document for reference when reading the technical rationale that follows.

Requirement R1 General Considerations

ESP Redefined

For backwards compatibility purposes, network border-based ESPs and EAPs remain a valid option for controlling the communications to and from BCS. However, virtualization technologies and models such as Zero Trust present equally effective methods that are not network border-based solutions. A Zero Trust model can implement more granular controls throughout a network on a per-access or per-session level.

Shared infrastructure and “Mixed Trust” Risks

For virtualized environments where SCI is used, a risk of side channel attacks exists. Virtualization allows disparate workloads of what could be differing impact to execute on the same CPUs and share the same memory (i.e., RAM). In this case the lower impact systems would become high water marked with the higher impact system through the PCA definition. This would in turn affect what requires protection by any associated ESPs. The risks associated with this scenario is mitigated in CIP-005-8 by either:

- Declaring the VCAs that share CPU or memory or are within the same ESP with a BCS as associated PCAs which will require they meet the security requirements (high water marking) that include ‘associated PCAs’; or
- Configuring the virtualization infrastructure to place VCAs of differing impact or trust levels into differing CPU and memory pools and configuring affinity controls to these pools such that hypervisors do not allow workloads in these differing pools to simultaneously exist or execute on the same hypervisor.

Assets with Multiple Classifications (PCA, EACMS, Intermediate System, SCI, etc.)

The definitions created to categorize Cyber Assets have historically included overlap. The definition of PCA was revised to include VCAs that share CPU or memory with a BCS. Additional definitions such as SCI and VCA will add to the possibility of additional instances of assets or systems meeting multiple definitions, such as SCI that are also EACMS.

These definitions are used in both the Applicable Systems column as well as within the requirement language. The fact that one asset or system may meet multiple definitions and therefor have multiple classifications does not pose a significant challenge as long as the Responsible Entity ensures that all requirements that pertain to ANY of the classifications are applied. In other words, if an asset or system meets both the SCI and the EACMS definition, requirements that apply to either categorization are applicable.

Firewall/Router on a Stick

A “firewall on a stick” or “router on a stick” is a reference to a networking design scenario by which a firewall or router has one single physical connection to a switch, but has access to multiple networks and broadcast domains by utilizing logical interfaces in combination with VLANs (Virtual Local Area Networks).

Devices on different VLANs are not able to communicate by default, so the primary purpose of this design is to allow for inter-VLAN routing enabling communication between devices which reside on different VLANs by way of the firewall or router.

As all traffic between these VLANs passes through the firewall or router it is uniquely positioned to restrict access and log traffic flows between devices on different VLANs facilitating compliance and the enforcement of security requirements.

This design allows an entity additional flexibility with respect to the creation of multiple Electronic Security Perimeters while minimizing the cost and number of physical networking devices required to provide proper levels of protection and isolation to each of the created Electronic Security Perimeters.

An entity may select this design to enable further isolation of distinct applications and systems from each other based on the assessed risk that they pose to the BES or to enhance their ability to control access to these systems.

Careful attention should be given to the isolation and access control of management interfaces that support this design as they have the potential to impact multiple Electronic Security Perimeters.

SDWAN

Software-Defined Wide Area Networks (SDWANs) are comprised of an underlay network and an overlay network.

The underlay network is what we traditionally refer to as our Wide Area Networks and is constructed with various telecommunications provider circuits and technologies, including Serial, MPLS, LTE, Cable Modem, DSL, etc.

The overlay network is a virtual network layer created upon the underlay network, generally via encrypted tunnels or other similar mechanisms. An overlay network may utilize one or more underlay networks via load balancing or network policies. The policies governing the overlay network may dictate parameters such as what traffic is permitted, what underlay to utilize based on the application type, what should be utilized as the primary path, and various other parameters.

SDWAN enables the construction of secured and isolated network paths with enhanced management and monitoring capabilities in addition to enabling additional services to and from the SDWAN such as VPN connectivity, firewall services, traffic inspection, and shared gateways.

This technology provides an increased level of control over Wide Area Networks while enhancing visibility, security, and redundancy, all while offering the potential to reduce the costs associated with providing connectivity between an entity's locations and assets.

Figure 1 depicts a typical SD-WAN where encrypted tunnels protect traffic between sites A to C as well as sites B to C.

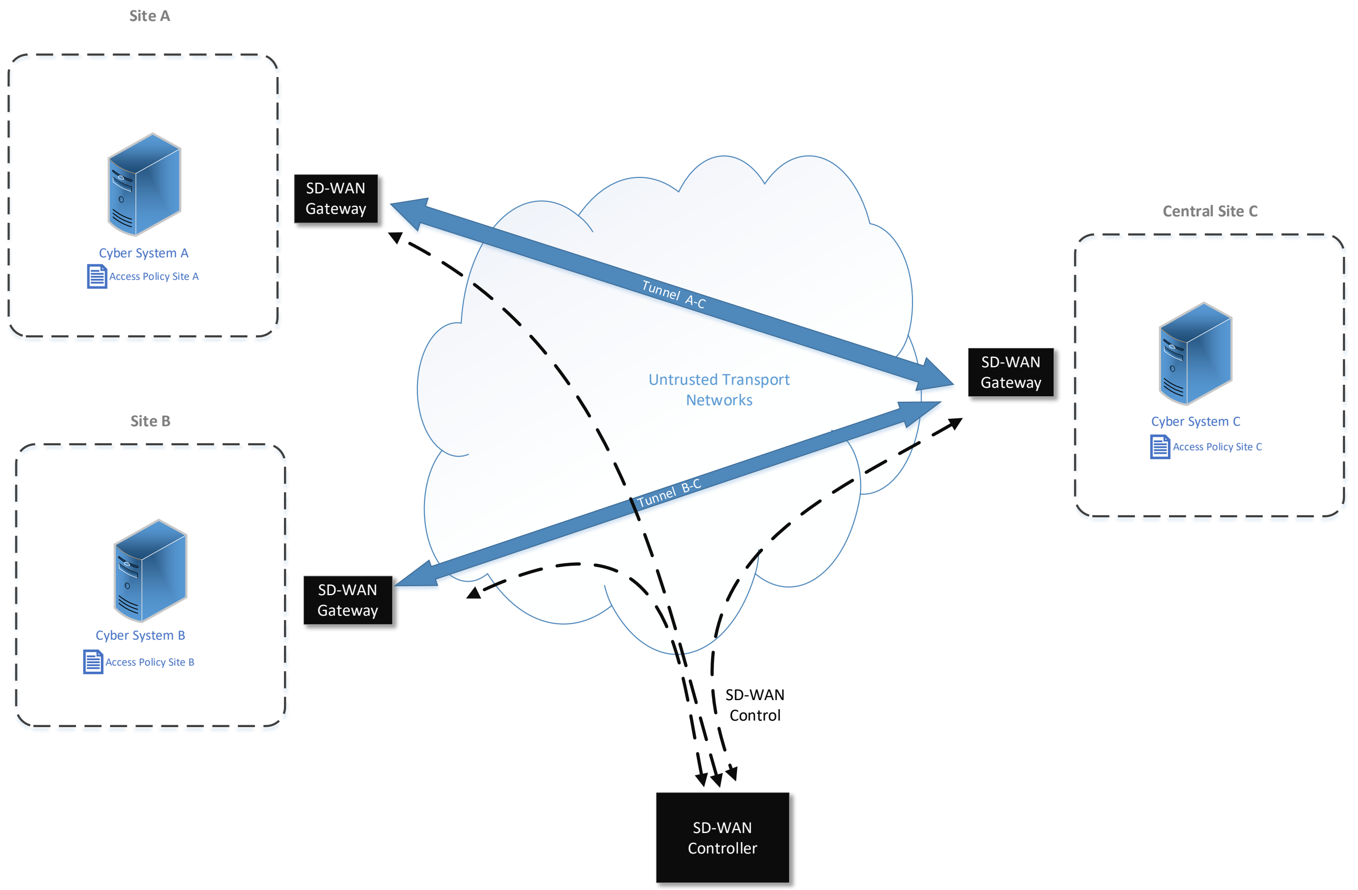


Figure 2 Typical SD-WAN

VXLAN

VXLAN is similar in concept to SDWAN in that it is a form of a Software Defined Network, but in the case of VXLAN the focus is on networks within the Datacenter as opposed to SDWAN which focuses on networks between Datacenters and other facilities.

VXLAN also utilizes the underlay and overlay terminology that we are familiar with given our review of SDWAN. The primary distinction is that VXLAN itself is the name of the overlay protocol utilized in this design and is the most common protocol used for overlay networks within a Datacenter.

The goal of VXLAN is to enhance the ability to segment network resources while also easing the burden of managing, automating, and orchestrating this segmentation by creating a virtual network that is agnostic of the physical network components supporting it.

The VXLAN protocol encapsulates Layer 2 Ethernet frames within Layer 3 UDP packets between devices comprising the design and allows for upwards of 16 million network segments to be created versus the traditional limit of 4094 VLANs. These network segments are identified with a VNI (VXLAN Network Identifier) which is synonymous with VLAN ID.

The components of the design that are capable of encapsulating and de-encapsulating the VXLAN protocol are referred to as VTEPs (VXLAN Tunnel Endpoints) and are commonly network switches or virtual machine hypervisors.

Physical devices and servers rely on switches to act as their VTEP whereas a virtual machine, hosted on VMWare ESX in this example, relies on the hypervisor as its' VTEP.

Figure 3 depicts a typical VXLAN where access control policies are implemented in the IP fabric.

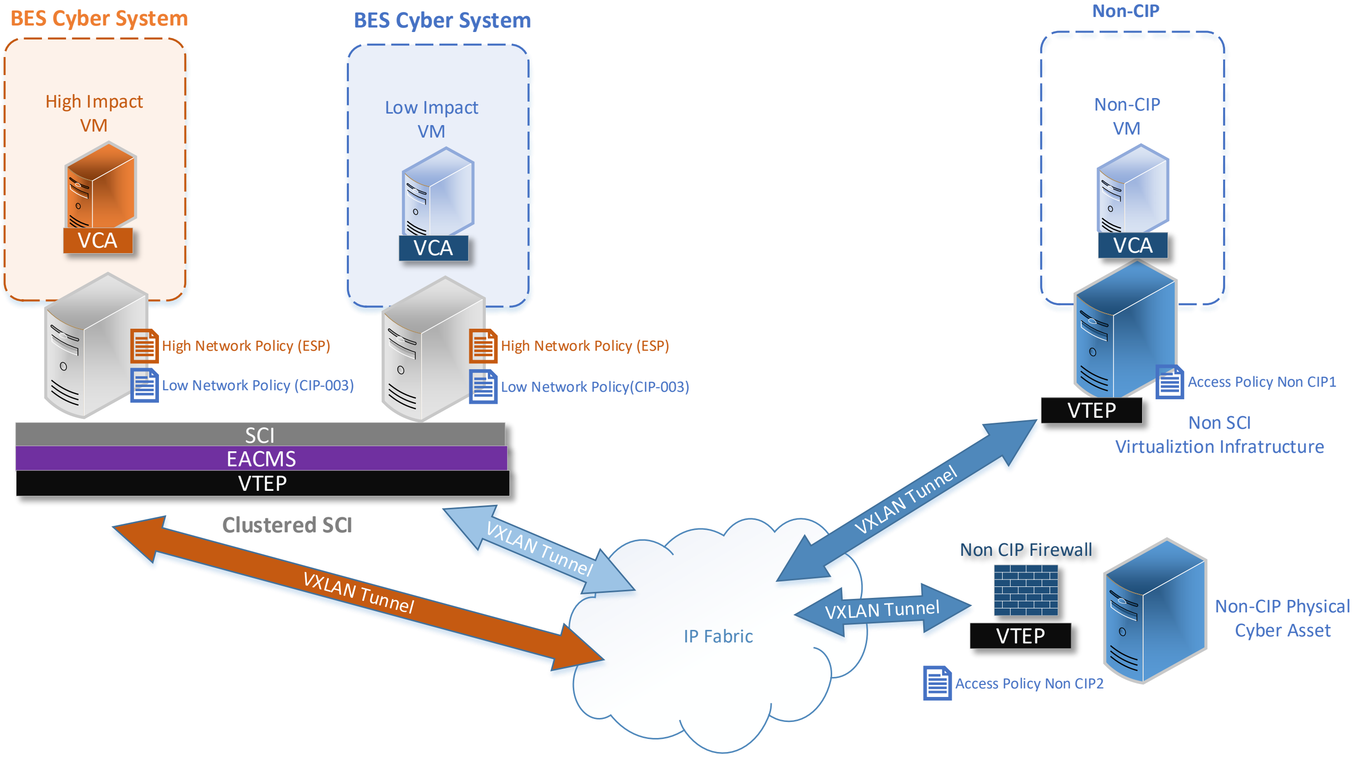


Figure 4 Typical VXLAN

VXLAN facilitates increasing the level of network segmentation within and between an entities Datacenters, while also enhancing their ability to automate and orchestrate the deployment of network resources. With this increased network segmentation an entity is granted more granular control over the flow of traffic and is given more opportunities to inspect that traffic to ensure appropriate levels of access control and protection.

Requirement R1

Rationale

Requirement R1 requires implementation of an ESP for BCS permitting only necessary communication through the ESP. However, there are other network security models available (such as zero trust) that can accomplish this security objective by controlling communications end-to-end at a more granular level than a network perimeter-based model. The definitions (ESP and EAP) and the changes to R1 allow entities the flexibility to implement different models that meet the security objective, or retain their current perimeter-based implementation.

Requirement R1 Part 1.1:

Rationale

This Requirement Part requires all high and medium impact BCS and their associated PCAs to be protected by an ESP. In recognition of non-perimeter based models, the language changed from “shall reside within” to “must be protected by”. Note, a PCA can now be defined by two different attributes of what they share with a BCS – not only network location, but also the sharing of CPU and memory from the underlying hypervisor(s) for VCAs. In the instance

that a VCA becomes an ‘associated PCA’ from its sharing of CPU or memory with a high or medium impact BCS, that associated PCA must also be protected by an ESP.

Note that this Requirement Part applies to all high and medium impact BCS without regard to external connectivity from the local network to other networks. This allows for the identification of PCAs and the scope of TCA connectivity even on isolated networks.

Requirement R1 Part 1.2:

Rationale

This Requirement Part changed to a security objective, rather than prescribing ERC must be controlled at an EAP. Virtualization technologies introduce additional methods to isolate systems. This requirement part no longer prescribes one method of controlling communications to Applicable Systems, and opens it up for alternative solutions.

This allows for other models such as zero trust architectures. Such models are not based on controlling communications at a Cyber Asset interface located on a network boundary. Communications can be authorized by software defined policy enforcement points throughout the infrastructure. In this model, network security is less topology-based and more policy-based (configurations and settings) and can be used to granularly protect communication at an individual system or even process or resource level.

While pure zero-trust architectures are an emerging model, the objective-based requirement also allows for hybrid models of various combinations of network border-based and zero trust architectures. As technology changes, this requirement and broadened ESP definition are flexible in how the objective is met.

The intent of “through the ESP” is to better incorporate future Zero Trust implementations where there is no “logical border surrounding a network” but instead Policy Enforcement Points at the accessed resource itself or as close to it as possible. In these instances that are designed to be perimeter-less, the concepts of “inside” and “outside” begin to fail and the SDT is removing those now to be better prepared for future technologies. The SDT asserts that even in traditional Layer 3 firewalls that define an ESP, the communications between systems that are encapsulated in packets go “through” the perimeter (ESP) in order to reach their destination.

The core security objective, of permitting only needed communications and denying all others by no longer prescribing this must be implemented at a Cyber Asset interface on a network border (an EAP), is retained. The intent of this Requirement Part is to control the ‘reachability’ of the Applicable Systems; filtering network communications *before* they reach the Applicable Systems and their OS, not as part of it. This is not to discourage the use of integrated host-based firewalls to further filter network traffic to a host.

Note that the requirement now explicitly includes “the reason for granting access”. Previously, this had been an implied part of the requirement based on the Measures.

The SDT had considered adding “physical isolation” to the Measure, but did not do so as the applicability explicitly includes ERC. Additionally, within the Measures, the SDT uses examples of VLAN and VXLAN configurations as evidence. These configurations could be used as methods to “Permit only needed routable protocol communications”, despite not being OSI layer routable protocols in and of themselves.

Time-sensitive communications between Protection Systems (i.e., digital relays) that use routable communication protocols are excluded. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by inserting an ESP and its controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles (sub-second response times) to protect BES assets. The SDT intent is a Responsible Entity using this technology is not expected to implement the electronic access controls in a situation where it would prohibit the proper function in the proper timeframe.

Requirement R1 Part 1.3:

Rationale

It is important to note that Requirement Part 1.2 is scoped to the Applicable Systems protected by (inside) the ESP while Requirement Part 1.3 is scoped to protect the Management Interface of the Cyber Assets creating and controlling the ESP and thus not protected by the ESP itself. These different scopes show the need for separate Requirements Parts. In addition, the separation into different Requirement Parts prevents a recursive requirement. Otherwise, each EACMS would require an EACMS creating an impossibility to implement.

The objective of this new Requirement Part is to protect ESP configurations and SCI configurations. The intent is preventing unauthorized changes to these important configurations by controlling what can connect to administrative interfaces for SCI and certain EACMS.

This can be done by permitting only needed communications to the Management Interfaces, denying all other communications, of the systems that are providing protection of BCS; namely SCI that is supporting an Applicable System from Part 1.1 (SCI isolates systems of different impact levels from each other) and certain EACMS that are controlling an ESP. This Requirement Part only applies to SCI and EACMS controlling an ESP, and not to the BCS itself).

These are vital controls performing the isolation/segmentation between systems of differing impact levels, and warrant protection of the Management Interface that could be used to compromise them.

Certain EACMS that can control access to an ESP are subject to this requirement. This includes those EACMS such as a firewall that is controlling an ESP, a centralized station administering firewalls controlling ESPs as well as a network switch configured with VLANs to isolate and segment traffic. These certain EACMS will need to have their Management Interfaces protected. The SDT intended to exclude EACMS not associated with control and ESP such as domain controllers that provide only authentication services. The SDT is aware of possible implementations where an authentication server is used to provide real-time control of ESP access on a per user basis. In these situations, the authentication server does fall within scope of an EACMS that controls access to an ESP.

The ‘per system capability’ is included in this Part in recognition that some Management Interfaces, such as “ILO” interfaces, may do inbound but not outbound traffic controls.

Requirement R1 Part 1.4:

Rationale

The SDT included “SCI supporting an Applicable System in this Part” to the scope of the requirement part to ensure that controls regarding Dial-up Connectivity are also applicable to VCAs and SCI; and ‘technical feasibility’ has been replaced with the ‘per system capability’.

Additionally, in order to maintain a decipherable Applicable Systems column, the SDT replaced the scoping phrase “with Dial-Up Connectivity” from the Applicable Systems column, with a reference to “if any” in the Requirement Language.

Requirement R1 Part 1.5:

Rationale

Known or suspected malicious communication detection is specific to routable protocol based traffic that enters or leaves the required ESP. Products available to implement this malicious communication detection are usually based on IP traffic (as defined in RFC 791 and upon which TCP and UDP reside). The SDT intended to exclude other data center communications protocols currently in use such as Fibre Channel, where it would not be possible to meet this requirement.

The requirement applicability was changed to the ESP instead of EAPs; lifting it to an objective level and keeping it from being a prescriptive ‘where’ that forces certain architecture. These protections at the ESP level do not preclude entities from accomplishing the security objective by implementing controls at the EAP level, but offer entities the flexibility to implement other methods at the ESP level.

The SDT considered adding SCI to the Applicable Systems; however, chose not to do so as this functionally may be provided by SCI, thus resulting in a recursive requirement issue. Note that the Management Interfaces of SCI are protected by Requirement R1.3. Entities may wish to implement malicious communications detection on these Management Interfaces of SCI.

Requirement R1 Part 1.6:

Rationale

Requirement R1 Part 1.6 was written to address the issue of “Super ESPs” with high or medium impact BCS at Control Centers that extend a single ESP beyond one PSP. This often applies to virtualized Control Center environments that implement network adjacency to allow workloads to automatically move from one physical location to another to increase BCS resiliency between primary and backup Control Centers.

The security objective is to protect the confidentiality and integrity of the data traversing communication links used to span a single ESP between multiple PSPs. This is especially important when portions of the transport are not within the Registered Entity’s control. Many encryption methods (such as IPSec and TLS) can fulfil this objective; however, some encryption methods fall short of providing both confidentiality and integrity controls.

This Requirement Part works in conjunction with the new 4.2.3.3 exemption in the CIP standards that exempts the Cyber Systems associated with such communication links since the data is required to be protected per this requirement. Also, the former CIP-006-6, Requirement R1, Part 1.10 has been removed and incorporated into this new 1.6 requirement part; consolidating the protections of an ESP and its components that extend outside of a PSP within one standard.

Communications equipment associated with communications links (e.g., equipment belonging to carriers) is exempted from the CIP standards with the 4.2.3.2 exemption. However that only applies to equipment between discrete ESPs. In this extended ESP situation where a single ESP spans multiple sites or PSPs, that exemption does not apply and the potential exists for data to traverse a connection that uses third-party communications equipment that is unprotected inside an ESP; hence the need to enforce confidentiality and integrity controls (such as encryption) on the data that traverses PSPs while within the same ESP to isolate any protected data from access through the communications equipment.

This consolidation also incorporates cabling and non-programmable communication components that are not PSP-protected, intending to protect data moving across the state as well as data traversing cabling that crosses the hall outside of the PSP. Note: the language specifically exempts the data that falls under CIP-012 Requirements in order to avoid the potential for double jeopardy as well as the time-sensitive protection or control functions as described in CIP-005-8 Requirement R1 Part 1.1 above.

The SDT had considered adding SCI to the Applicable Systems; however, chose not to do so as this functionality may be provided by SCI, thus resulting in a “hall of mirrors” issue.

Requirement R2:

General Considerations for Requirement R2.

External Routable Connectivity (ERC) and Interactive Remote Access (IRA)

The ERC and IRA definitions have been updated in order to:

1. Incorporate new models such as Zero Trust where a security perimeter is not necessarily a network perimeter and ESPs become very granular based on policies that can be established at “people to resource” levels rather than IP address levels.
2. Recognize those Cyber Systems that are of an increased risk due to their “reachability” via ERC and that have IRA available to them even if they are serial-only, non-routable devices.
3. Continue to limit scope of Requirement Parts to BCS with ERC and not those that have connectivity such as non-routable serial leased circuits.

The V5TAG transfer document in the SDT’s scope includes the issue of a BES Cyber Asset (BCA) that only uses non-routable protocols over a serial port. These BCAs are not connected to a network with a routable protocol themselves and therefore can be considered to not be within an ESP and thus not have ERC. However, these BCAs can have interactive user access using those serial connections. The SDT’s intent is to clarify that IRA can occur to a device with only a serial, non-routable connection through IP-to-serial conversions and be subject to CIP-005-8 Requirement R2. For example, the intent is to clearly cover situations where a serial-only, non-routable BCA, such as a digital relay in a substation, has its serial communication from a ‘console port’ converted to IP or other routable protocols thus allowing IRA from users outside the substation to use a routable protocol to interact with the serial device and to require the CIP-005-8 Requirement R2 protection for that IRA.

Due to the inclusion of serial based connections into the revised definition of IRA, other CIP requirements (i.e., CIP-004) have been revised to conform. Entities should review serial/IP converters that are currently being used for remote access.

The SDT removed the requirement-style language “The Intermediate System must not be located inside the Electronic Security Perimeter” from the Intermediate System definition in favor of a clarified objective in CIP-005-8 Requirement R2 that all IRA must be *through* an Intermediate System. Requirement R2 Part 2.6 was added to objectively address the location of the Intermediate System.

See the “*CIP Definitions and Exemptions Technical Rationale*” document for further explanation of the changes to the R2 related definitions.

Requirement R2 Part 2.1:

Rationale

Applicable Systems was updated to include SCI to ensure the same safeguards for remote access methods exist for SCI supporting an Applicable System within the Part as they do for the high and medium impact BCS and associated PCA hosted on that SCI. Backwards compatibility is retained for entities that do not use SCI. Please note that there may be situations where an Intermediate System is implemented as a VCA on SCI. The SDT intends that applicability for SCI is to ensure that the objectives of Requirement R1.3 are met such that the Management Interfaces of SCI are appropriately protected. VCAs are not considered part of SCI and therefore could be used to access a Management Interface of SCI.

The requirement language was simplified, and definitions for IRA and Intermediate System have been updated. Please note that the definition of IRA was changed to include serial communications that are converted to/from routable protocols by the Responsible Entity. This change maintains backwards compatibility except where serial connectivity and routable protocol conversion is being used for IRA.

Requirement R2 Part 2.2:

Rationale

The “Applicable Systems” scope was changed to “Intermediate Systems used to access Applicable Systems in Part 2.1”. This clarifies this requirement is associated with the IRA communications between an Intermediate System and the remote clients, as opposed to between the Intermediate System and the BCS. This is important so that it does not require encryption through the ESP to the BCS which would hinder monitoring and inspection.

The requirement was changed from a specific technical-based requirement for encryption to an objective-based requirement to protect confidentiality and integrity of the IRA session between the Intermediate System and the remote client (with encryption as a primary example). The proposed language accounts for the possibility that other equally effective methods could be developed and deployed. This objective also keeps methods from being used that are merely obfuscation methods (XOR, ROT13, etc.) or deprecated encryption methods (DES with 56-bit keys) that no longer meet the objective to protect the confidentiality and integrity of the IRA session.

The changed requirement is backwards compatible except where deprecated encryption methods are in use.

Requirement R2 Part 2.3:

Rationale

Applicable Systems was changed to “Intermediate Systems used to access Applicable Systems of Part 2.1”. This clarifies this requirement is associated with the Intermediate System itself, and where the requirement for multifactor authentication should be applied (multi-factor authentication to the Intermediate System).

Note that the wording of the requirement was updated to specially apply to IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System. This was previously implied.

Requirement R2 Part 2.4 – 2.5:

Rationale

The applicability and requirements have not changed.

Requirement R2 Part 2.6:

Rationale

This is a new requirement that applies to Intermediate Systems. The intent of this new requirement is to further protect the BCS from the Intermediate System by reducing the attack surface between the two. It is important to note that a virtualized Intermediate System (VCA) hosted in such a way that it can share CPU and share memory with a BCS will also meet the definition of PCA and become an ‘associated PCA’ of the BCS. CIP-005 R1.1 requires that PCA to be within an ESP, in conflict with this requirement. This is by design, and thus a VCA performing the function of an Intermediate System must not share CPU or memory with the BCS it is controlling access for. This is due to the access granted to the less trusted side of the Intermediate System and the risk for side-channel attacks to other VCAs sharing the same CPU and memory. Entities must therefore use affinity rules or some other means to keep Intermediate System VCAs from sharing the same CPU and memory as a BCS or its associated PCAs.

Figure 5 depicts an Intermediate System VCA where an affinity ruleset prevents the sharing of CPU or the sharing of memory with a BES System by ensuring these systems run on different on the hypervisor.

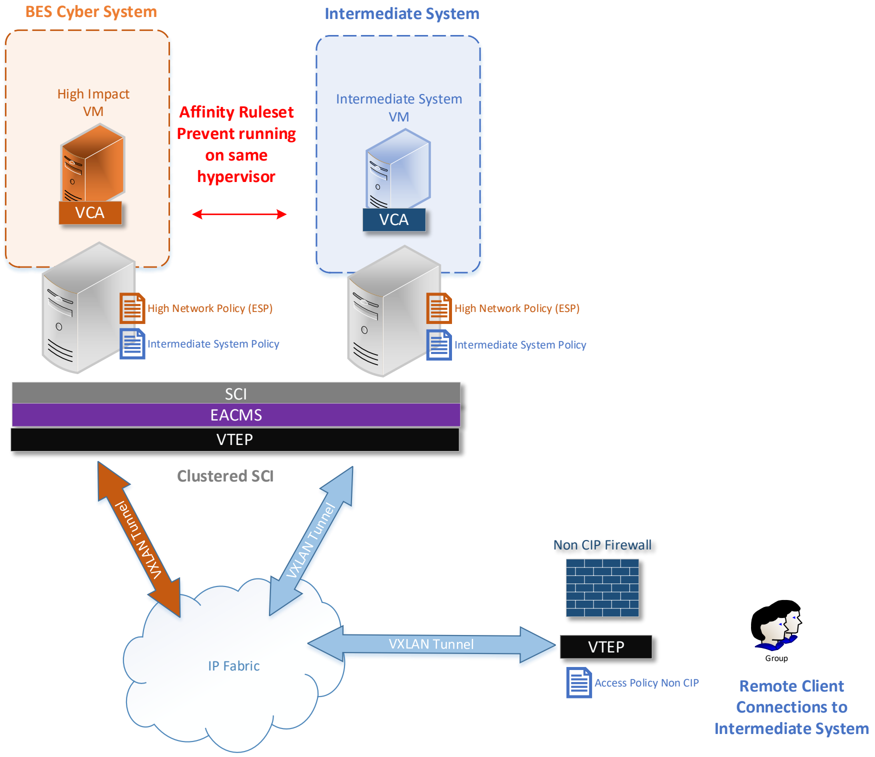


Figure 6 Affinity Rules - Intermediate System does not share CPU or share memory with BES Cyber Systems

Requirement R2 Part 2.7:

Rationale

This is a new requirement that applies to Intermediate Systems. The intent of this new requirement is to further protect the BCS from the Intermediate System by reducing the attack surface between the two. Intermediate Systems have an externally accessible interface that may be used by external parties such as vendors or entity support staff using IRA across an Internet connection to support a remote site. Since Intermediate Systems by nature provide IRA from a less-trusted network and are accessible from yet-to-be authenticated users (in order to authenticate them), a degree of separation from the higher-trust systems they are protecting is necessary in case the Intermediate System is compromised. Previously, this risk was addressed within the glossary definition of Intermediate System ("…must not be located inside the ESP") instead of within an actual requirement. The SDT removed this from the definition and included a security objective in CIP-005-8 Requirement R2 Part 2.7 to require that routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.

It is important to note that the SDT does not intend to prescribe architecture to the point of what Cyber Asset or Virtual Cyber Asset a function may reside. For example, some "security appliances" that have firewall/EAP capability also have separate functionality within them that can perform part of the Intermediate System function. Historically this definition has stated "must not be located inside" which allowed for "outside or ON" the ESP. The SDT does not want to preclude architectures where at least some portion of the Intermediate System functionality may execute on the EAP.

Figure 7 depicts an Intermediate System running on non SCI infrastructure. Network connections from the Intermediate System to the BES Cyber Systems must pass through the ESP protecting those systems. In this case, access control policies, implemented on SCI are used to control network connections.

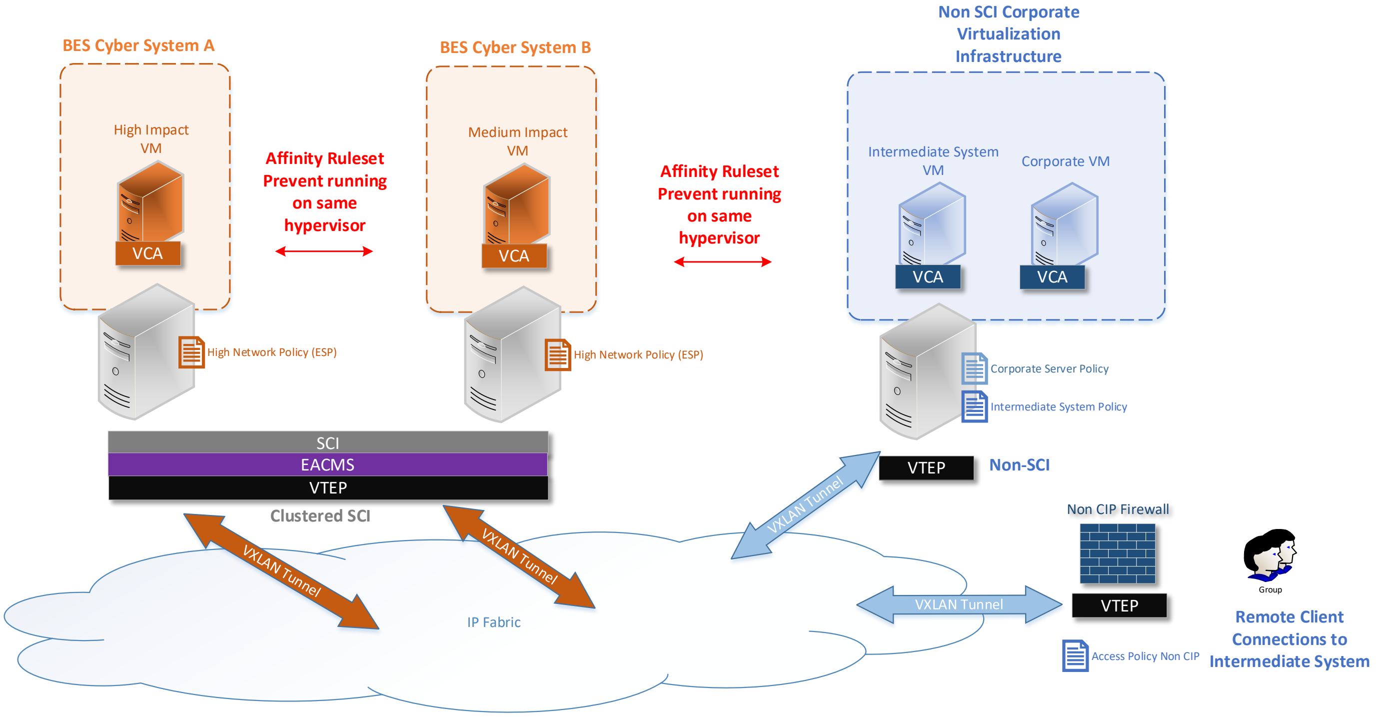


Figure 8 Intermediate System must connect through the Electronic Security Perimeter protecting the BES Cyber Systems

Requirement R3

Rationale

The Applicable Systems section of CIP-005-8 Requirement R3 was updated to include SCI to ensure the same safeguards for vendor-initiated remote connections exist for the applicable SCI. Backwards compatibility is retained for entities that do not currently use SCI.

Background Section from Reliability Standard CIP-005-7

The section 6. Background has been retired. removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BCS and require a minimum level of organizational, operational and procedural controls to mitigate risk to BCS.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BCS. For example, a single training program could meet the requirements for training personnel across multiple BCS.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

Technical Rationale for Reliability Standard CIP-005-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The ESP serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.

But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e., system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the “first line of defense within an Industry Control System (ICS) network environment”. The compromise of those devices that control access management could provide an outsider the “keys to the front door” of the ESP where BES Cyber Systems reside. An intruder holding the “keys to the front door” could use those “keys” to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability

Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[1].

NERC's final report on "*Cyber Security Supply Chain Risks*", states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks*" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

---

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains an as-is "cut and paste" of the former Guidelines and Technical Basis (GTB) from Reliability Standard CIP-005-6 Technical Rationale to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an “Associated Protected Cyber Asset” of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually ‘command and control’ hosts on the Internet, or compromised ‘jump hosts’ within the Responsible Entity’s other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT’s intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity’s address space. The SDT’s intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and ‘deny by default’ type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear ‘perimeter type’ security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions (“TFEs”) rather than increased security.

As for dial-up connectivity, the Standard Drafting Team’s intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.

But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

Exhibit E-5

CIP-006-7

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Physical Security of BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-006-7

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-006-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-006-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-006-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-006-7 to shorten applicability statements within the body of CIP standards by replacing some terms with the defined acronym for that term:

"BCS" has replaced "BES Cyber System".

"ERC" has replaced "External Routable Connectivity".

"PSP" has replaced "Physical Security Perimeter".

"PACS" has replaced "Physical Access Control Systems".

Requirement R1

Rationale

The SDT made conforming changes to Applicable Systems for virtualization such that protections must be afforded to SCI for relevant Requirement Parts.

<u>Applicable Systems</u>:
Requirement R1 Part 1.1-1.9: the SDT added "SCI supporting an Applicable System in this Part.

<u>Per System Capability vs Technical Feasibility</u>:
Requirement R1 Part 1.3: The SDT chose to remove the reliance on a Technical Feasibility Exception in favor of the updated term "per system capability."

<u>Consolidation</u>:
Requirement R1 Part 1.10: The SDT deleted Requirement R1 Part 1.10 from CIP-006-7 because requirements to protect the data traversing communication links used to span a single ESP between PSPs is incorporated into CIP-005-8 Requirement R1 Part 1.6.

Requirement R2

Rationale

The SDT has include the CIP Exceptional Circumstances within the main R2 requirement text so that it applies to all requirement parts.

The SDT made conforming changes to Applicable Systems for virtualization such that protections must be afforded to SCI for relevant Requirement Parts.

<u>Applicable Systems</u>:
Requirement R2 Part 2.1-2.3: the SDT added "SCI supporting an Applicable System in this Part"

Former Background Section from Reliability Standard CIP-006-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-006-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-006-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the PSP.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A logbook or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more PSPs, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System, but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where these cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the PSP to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the PSP. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a PSP (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any PSPs protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit E-6

CIP-007-7

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — System Security Management

Technical Rationale and Justification for Reliability Standard CIP-007-7

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-007-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-007-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-007-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale.pdf" for reference when reading the technical rationale that follows.

General Considerations

Requirement R1

General Considerations for Requirement R1

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To clarify treatment of virtualization concepts in CIP-007-7, the SDT added “SCI supporting an Applicable System in this Part”. This approach keeps the SCI applicability parallel to each existing variant of Applicable Systems in the same Requirement Part (i.e., Medium impact BCS vs. Medium impact BCS with External Routable Connectivity (ERC) vs. Medium impact BCS at Control Centers etc.)

Change Rationale Requirement R1:

The SDT has changed the name of the R1 table to “System Hardening” to clearly reflect the security objective of the entries in the table, which is to reduce a systems’ attack surface. The parts of this requirement do this by:

- limiting network access to only needed routable protocol network accessibility (i.e., logical ports or services),
- limiting access to physical I/O ports (i.e., USB, network, console ports) to only what is necessary, and
- limiting the shared hardware (CPU and memory resources) attack surface between certain groups of VCAs on SCI.

As R1 is broader than only ports and services, the table name was changed to reflect this. The SDT notes that this is merely a label on the Requirement Parts table, linking it to the main Requirement 1 language above it, and does not change or imply any other Requirements or Requirement Parts.

The SDT chose to include “SCI supporting an Applicable System in this Part” language in the Applicable Systems column of the requirement to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCA.

Change Rationale Requirement R1 Part 1.1: Requirement R1 Part 1.1 requires “disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability”. The SDT updated the Requirement Part language to state a security objective concerning “*routable protocol network accessibility*” as opposed to “ports and services”. As this is a new phrase, the intent of this phrase with some examples and rationale for this change is as follows.

> ***Routable protocol network accessibility*** - The objective of this phrase in the Requirement Part is to reduce the attack surface on an applicable system by preventing any unnecessary accessibility to the system over a network using routable protocols. “Accessibility” as used in R1.1 is at the routable protocol network level and does not include physical access, logon to the physical console, code on TCA/RM, etc. Port numbers (TCP/UDP) are at times the best way to track this accessibility, at other times documenting enabled services is better. For example, reducing network accessibility in the physical underlay of SCI between hypervisors or on fabric-based networks may be best performed at a *services* level; turning off or disabling virtualization services that are not needed, rather than documenting the often proprietary and dynamic port numbers which may be of little value. However, in the overlay where an entity may be hosting a database server VCA, it may be easier to show that network accessibility on that VCA is limited to SQL server and remote admin enabled port numbers. In Zero Trust Architectures (ZTA), it may be neither ports or services, but instead a “user to tagged workload” level access control policy where accessibility is described and protected at a more granular, yet higher level than a port #, enforced at a Policy Enforcement Point (PEP) on the applicable system. The SDT has moved to this objective language to avoid prescribing only one way to perform and document network accessibility in all these various scenarios and implementations. In addition, it is limited to routable protocol network accessibility such that non routable network communications (e.g., SAN over Fiber Channel) do not fall within scope of the Requirement Part. The objective is to know the ways a system

can be accessed from the network via routable protocols and have no unnecessary attack surface from that perspective.

In this Requirement Part, the SDT used the verbs "Disable or prevent". In some cases, the entity may be able to disable a service or remove/uninstall software that is providing unneeded network accessibility to the applicable system. In other cases, the entity may not be able to disable a service, but can prevent access to it in another layer, such as the underlying OS with a host-based firewall, a PEP, or other means of filtering traffic. In instances where the entity can do neither (e.g., a firmware-based 'black box' device with limited configuration capabilities), the SDT chose to add 'per system capability' to make the requirement conditional on the ability of the applicable system to meet it, if the entity can show that it is incapable.

The SDT also added the clarifier "on each Applicable System" to indicate that the intent of this requirement is for an entity to perform the configuration actions ***on*** each Applicable System, hardening the system from its routable protocol network peers rather than having a single method such as an EAP network firewall rule that would disable such accessibility for a group of Applicable Systems on a network. In other words, merely filtering a port/service on a firewall at an ESP network boundary (CIP-005 R1 controls) does not meet the intent of CIP-007 R1.

Change Rationale Requirement R1 Part 1.3:

Requirement R1 Part 1.3 is a new requirement intended to apply security controls in Shared Cyber Infrastructure scenarios to mitigate the risk of hardware-based vulnerabilities between groups of Applicable Systems of differing impact categorizations. This requirement addresses these vulnerabilities at the CPU and memory level (e.g., Downfall, Inception, Spectre, Meltdown, Rowhammer) that could allow for compromise across processes simultaneously executing on the same shared hardware. Virtualization technology typically has "affinity" controls that can be used to tag VCAs by their impact category and then configure affinity rules such that hypervisors do not instantiate or move VCAs of differing trust levels to the same CPU or memory resources at the same time. Note the requirement excludes shared storage resources, although included in the definition of SCI. The SDT intent is it is allowable to have logical disks attached to systems of differing impact categorization stored in the same SAN for example, and since these storage solutions have internal CPU and memory, which is not the intended object of this requirement.

Note that the SCI definition covers *only* those portions of entity's virtualization infrastructure that support systems of differing impact levels. As VCAs that share the same CPU or memory with any part of the highest rated BCS are "Associated PCAs", this requirement is only needed to cover instances where different impact categorizations are supported and the entity wishes to keep other VCAs from becoming "associated PCAs', thus maintaining the separation by impact category. This may occur when part of the same SCI supports different BCS and the entity does not wish to high watermark all the BCS together, but instead employ affinity rules to prevent VCAs that are high or medium impact from being instantiated or moved to CPU and memory resources where other VCAs are executing.

For example, this requirement would apply where the same SCI supports both a high impact BCS on one part of a virtualization cluster and a low impact BCS on a different part of the virtualization cluster. The proper use of host affinity controls would not require the low impact BCS to be considered an "associated PCA" of the high as long as:

1. the low impact BCS is not in the ESP of the high impact BCS, and
2. controls are in place to prevent the SCI from executing these BCS on the same CPU and memory resources.

As an example, if an entity has a substation intelligent electronic device (IED) management system that is used as an EACMS for medium and low impact BCS in a single VCA, it is an associated EACMS of the medium impact BCS and protected as such. It can therefore execute on hypervisors with other medium or high impact BCS. If it is implemented as two separate VCAs, one for medium impact IEDs and another for low impact IEDs, then the low impact one cannot execute on the same hypervisor as the medium impact one, unless it is categorized as an "associated PCA" of the medium BCS as well. If the entity wishes to have it remain as low impact those two VCAs sharing the same CPU or memory resources would not meet this requirement. In situations where high or medium impact VCAs are allowed to execute on the same CPU or memory resources with VCA's of other impact levels and those other VCA's are inadvertent PCAs, this requirement is a single place for that violation rather than every requirement that has PCA in the scope.

Requirement R2

Change Rationale Requirement R2:

The SDT chose to include the "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA(s) used in applicable BCS, EACMS, PACS or PCA.

The SDT made conforming changes where necessary with Requirement R2 to remove reliance on the Cyber Asset term, choosing to reference the Applicable Systems instead.

Additionally, the SDT chose to insert the word "cyber" as a clarifier to security patches for consistency with the term used in R2.1.

Backward Compatibility

CIP-007-7 Requirement R2 retains backward compatibility for entities that do not utilize SCI.

The SDT intends that entities take full advantage of their virtualization infrastructure in order to ease the overhead associated with patch management. While many of the entity's existing processes will remain the same, (such as those associated with tracking the source of cyber security patches, evaluation of the applicability of available patches and mitigation plans for those applicable patches that cannot be installed) new or modified processes around the installation of patches can be used (for example, parent images, remediation VLANs, etc.).

Parent Images

One of the interesting nuances of virtualization is the concept of parent/child relationships.

Some VCAs utilize a "parent image" type methodology where a specific VCA (operating system and software) is merely a child instance of a parent image. In such cases, the application of cyber security patches to the parent image applies those changes to any children instantiated from that image. As there may be many dynamic child instances, the administrative overhead associated with patching of those child instances can be greatly reduced. The intent is that entities would track and document the R2 cyber security patching requirements at the parent image level rather than attempting to track and document patching for each individual VCA instantiated from the parent image.

Dormant Instances

There are times when a VCA may not be in use and, as a virtual instance, may be shut down to free its resources since it can be easily instantiated when needed. Thus, VCAs are unlike physical Cyber Assets that are up and running continuously and can receive applicable patches, software updates, configuration updates, etc.

Leveraging the built-in virtualization features allows idle resources to be reassigned to tasks at hand without incurring additional overhead of tracking which dormant virtual instances require patching. Dormant virtual instances are just files with the saved state of the VCA. Dormant instances are not VCAs themselves nor Applicable Systems until they become active instances again.

Where a dormant virtual instance is also the child instance of a parent image, the application of security patches to the parent image will also make the same changes automatically when needed to any out of date dormant child virtual instances when they are restarted.

In most cases, a dormant virtual child instance is made active again on a remediation type network where any missing security patches (compared to the parent image) are automatically applied before it is placed back into active service.

Saved Images

Similar to dormant child images, saved child images or snapshots may be also used as functional backups for CIP-009 purposes in order to provide fast restoration and better availability. If an active VCA becomes corrupted, a saved image can be made active where the application of any missing security patches (compared to the parent image) can be automatically applied, through remediation, before being placed back into active service. However, the SDT's intent is that VCA images that are used for backup purposes would not be subject to patching, as the backup may be needed to recover from a failed patch or if later discovered that a patch has negatively affected functionality.

Requirement R3

Change Rationale Requirement R3:

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA.

Requirement R4

Change Rationale Requirement R4:

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA.

Change Rationale Requirement R4 Part 4.1:

The SDT determined the entire structure of the "at the BCS level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)" language could be simplified to "per system capability" since the Applicable Systems column clarifies what systems are included.

Additionally, the SDT chose to insert the word "security" as a clarifier to which events are to be logged.

Change Rationale Requirement R4 Part 4.2:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the "Cyber Asset" term, as well as the ambiguity that would have existed if the term "BES Cyber System" were left in place while the Applicability Column included SCI.

Change Rationale Requirement R4 Part 4.3:

The SDT clarified the retaining of applicable "security" event logs, as that is what is identified in Part 4.1.

The SDT also chose to remove the reliance on a TFE from Part 4.3 in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

Requirement R5

Change Rationale Requirement R5:

The SDT chose to include “SCI supporting an Applicable System in this Part” language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCAs.

Change Rationale Requirement R5 Parts 5.1, and 5.6 – 5.7:

The SDT chose to remove the reliance on TFE in favor of the updated term “per system capability”. The SDT contends that the term still requires an entity to document the limit to the system’s capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

Change Rationale Requirement R5 Part 5.4:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the “Cyber Asset” term, replacing it with a per “system” capability.

Change Rationale Requirement R5 Part 5.5:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the “Cyber Asset” term, replacing it with a reference to the Applicable Systems.

Former Background Section from Reliability Standard CIP-007-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-007-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-007-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

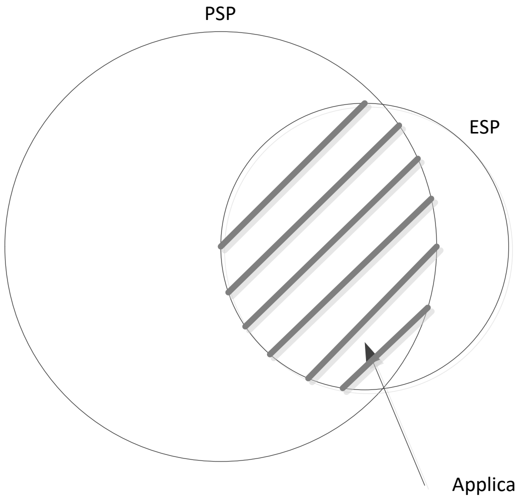
- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:

Location of Nonprogrammable Communication Components



Applicability of CIP-007-6 R1, Part 1.2 for Nonprogrammable Communication Components

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media (“transient devices”) in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System’s ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a ‘false positive’ could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC’s reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity’s control (i.e. as part of the telecommunication carrier’s network).

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit E-7

CIP-008-7

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security – Incident Reporting and Response Planning

Technical Rationale and Justification for Reliability Standard CIP-008-7

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-008-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-008-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 – Requirement R4

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-008-6 to align incident reporting and response planning requirements with the virtualization changes and protections for Shared Cyber Infrastructure (SCI) by adding "SCI supporting an Applicable System in this Part" to each of the Parts in Applicable Systems for Requirement R1 – Requirement R4.

Requirement R4

Rationale

The Project 2016-02 SDT made updates to reflect the change from the National Cybersecurity and Communications integration Center (NCCIC) to its successor organization Cybersecurity & Infrastructure Security Agency (CISA), and deleted the historical footnote in favor of deference to the Requirement language, which already states "or their successors".

Former Background Section from Reliability Standard CIP-008-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST")

Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

Medium Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

Technical Rationale for Reliability Standard CIP-008-6

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-6. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-008-6 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 19, 2018, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 848. In this Order FERC directed the North American Electric Reliability Corporation (NERC) to "develop and submit modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access and Control or Monitoring System (EACMS)." (Order 848, Paragraph 1)

In response to the directive in Order No. 848, the Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require Responsible Entities to implement methods augmenting the mandatory reporting of Cyber Security Incidents to include: "(1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report included specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT)." (Order 848, Paragraph 3)[1]

New and Modified Terms Used in NERC Reliability Standards

CIP-006-6 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms:

Cyber Security Incident

A malicious act or suspicious event that:

- *For a high or medium impact BES Cyber System, compromises, or attempts to compromise the, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or*
- *Disrupts, or attempts to disrupt, the operation of a BES Cyber System.*

In response to FERC Order 848, Paragraph 1, the SDT modified the Cyber Security Incident definition to include Electronic Access Control or Monitoring Systems (EACMS) associated with high or medium impact BES Cyber Systems, in response to the Order.

The addition of high and medium impact BES Cyber Systems considers the potential unintended consequences with the use of the existing definition in CIP-003-7. It also provides clarity that only low impact BES Cyber Systems are

---

[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

included within the definition. ESP or EACMs that may be defined by an entity for low impact BES Cyber Systems are not part of the definition.

An attempt to disrupt the operation of a BES Cyber System is meant to include, among other things, a compromise of a single BES Cyber Asset within a BES Cyber System. For example, malware discovered on a BES Cyber Asset is an attempt to disrupt the operation of that BES Cyber System.

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:

- *A BES Cyber System that performs one or more reliability tasks of a functional entity;*
- *An Electronic Security Perimeter of a high or medium impact BES Cyber System; or*
- *An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber Systems.*

The Reportable Cyber Security Incident definition was modified to comply with FERC Order 848. In response to Paragraph 54 of the Order, the SDT modified the definition to include incidents that compromised or disrupted an ESP or an EACMS. The team also added the qualifying clause for “A BES Cyber System that performs one or more reliability tasks of a functional entity” to clarify what was compromised or disrupted, thus not extending the scope to Protected Cyber Assets (PCAs). In response to comments, the SDT left the entire definition of BES Cyber system in Reportable Cyber Security Incident to provide clarity.

It is also important to understand the relationship between the two definitions, the requirement language, and how they work in concert to classify events and conditions at varied levels of significance as the Registered Entity executes its process and applies its defined criteria to determine if reporting is required.

Electronic Access Control or Monitoring Systems (EACMS)

The drafting team spent significant time discussing this topic among its members, through industry outreach, and with FERC staff. The team believes by not specifically referencing the five functions in Order 848, we have reduced complexity and made compliance with the Standard achievable. The drafting team asserts that the five functions are equivalent to the current definition of EACMS in the NERC Glossary of Terms. If entities have questions about application of the EACMS definition, the drafting team advises entities to discuss those questions directly with NERC.

Requirements R1, R2, and R3

General Considerations for Requirement R1, Requirement R2, and Requirement R3

FERC Order 848, Paragraph 1, directs modifications to Reliability Standards to require reporting of incidents that compromise, or attempt to compromise a responsible entity’s ESP or associated EACMS. The intent of the SDT was to minimize the changes within CIP-008 and address the required modifications. To do this, the SDT added “and their associated EACMS” to the “Applicable Systems” column for Requirements R1, R2, and R3.

To add clarity to “attempts to compromise,” the drafting team created Part 1.2.1 to require entities to establish and document their process to include criteria to evaluate and define attempts to compromise. This requirement maps to Requirement 4 Part 4.2, which requires entities to use that entity-defined process for determining which incidents entities must report.

The use of the language describing Cyber Security Incident(s) as being “an attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the ‘Applicable Systems’” column for the Part is meant to clarify which Cyber Assets are in scope for attempts to compromise reporting by entities. This language is used throughout the standard.

Moving Parts of Requirement R1 to Requirement R4

To minimize the changes to Requirement R1, the SDT created Requirement R4 and consolidated all the CIP-008-6 reporting requirements. The SDT deleted Requirement R1 Part 1.2 reporting requirements from CIP-008-5, and moved them to Requirement R4 for this purpose.

Inclusion of “Successor Organizations” throughout the Requirement Parts

The SDT recognizes that organizations are constantly evolving to meet emerging needs, and may re-organize or change their names over time. The ICS-CERT has completed its name change to the National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems. The E-ISAC previously re-branded its name and may again in the future. By following Requirement R4 references to E-ISAC and NCCIC with “or their successors” the SDT is ensuring that Requirement R4 can be implemented even if the names of E-ISAC and NCCIC change or a different agency takes over their current roles.

Requirement R4

General Considerations for Requirement R4

Requirement R4 is a new requirement focused on mandatory reporting of Reportable Cyber Security Incidents and includes attempts to compromise systems in the “Applicable Systems” column. Previously, CIP-008-5 defined reporting requirements for Reportable Cyber Security Requirements (Requirement R1 Part 1.2) only.

Required Reportable Incident Attributes

Requirement R4.1 specifies that initial notifications and updates must include three attributes: 1) functional impact, 2) attack vector used, and 3) level of intrusion achieved or attempted. These attributes are taken directly from the Order. (FERC Order No. 848, paragraph 89).

The SDT understands that some or all of these attributes may be unknown at time of initial notification. To account for this scenario the SDT included “to the extent known” in the requirement language. There is an expectation that update reporting will be done as new information is determined or unknown attributes become known by the entity. There could be cases, due to operational need, that all the attributes may never be known, if this case presents itself that information should be reported.

Methods for Submitting Notifications

Requirement R4 Part 4.2 allows responsible entities to submit notification using any method supported by E-ISAC and NCCIC. The SDT did not prescribe a particular reporting method or format to allow responsible entities’ personnel to focus on incident response itself and not the method or format of reporting. It is important to note the report must contain the three attributes required in Requirement R4 Part 4.1 as they are known, regardless of reporting method or format.

Notification Timing

Requirement R4 Part 4.2 specifies two timelines for initial notification submission; one hour for Reportable Cyber Security Incidents; and end of next calendar day for attempts to compromise systems in the “Applicable Systems” column. Paragraph 3 of FERC Order No 848 directly states that reporting deadlines must be established. Paragraph 89 further states that “timelines that are commensurate with the adverse impact to the BES that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.”

- *Reportable Cyber Security Incidents* – The SDT wrote Requirement R4 Part R4.2 to use a one hour deadline for reporting of these events because incidents in this category include successful compromise of ESP(s), EACMS, or BES Cyber System(s). One hour is referenced directly in FERC Order No 848 paragraph 89 and is also the current reporting requirement in CIP-008-5.
- *Cyber Security Incident that was an attempt to compromise one or more systems identified in the “Applicable Systems” column* - Due to the lower severity of these unsuccessful attempts at compromising ESP(s), EACMS, or BES Cyber System(s), the SDT proposed a longer reporting timeframe. The intent behind

> the decision to add "By the end of the next calendar day" (11:59 pm local time) was to give responsible entities additional time to gather facts prior to notifications for the less severe attempts to compromise Applicable Systems. It is important to note that compliance timing begins with the entity's determination that attempt to compromise meets the process they defined in Requirement R1 Part 1.2.1.

The SDT understands initial notification may not have all the details when first submitted. It is expected, however, that information that has been determined is reported within the notification deadlines. Additionally, it is important to note the wording in Requirement R4 Part 4.2. The "compliance clock" for the report timing begins when the Responsible Entity executes its process from Requirement R1 Part 1.2.1 and a determination has been made that the type of incident which has occurred qualifies as reportable.

Technical rationale taken from the Guidelines and Technical Basis (GTB) CIP-008-5 Requirement 1 provides additional justification for the SDT to maintain the one hour timeframe for Reportable Cyber Security Incidents.

> *"The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."*

In 2007, the Electricity Information Sharing and Analysis Center (E-ISAC) was known as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Its voluntary procedures required the reporting of a cyber-incident within one hour of an incident. CIP-008-1 required entities to report to the ES-ISAC.

In FERC Order No. 706[2] (July 18, 2008), the Commission concluded that the one-hour reporting limit was reasonable [P 663]. The Commission further stated that it was leaving the details to NERC, but it wanted the reporting timeframe to run from the "**discovery**" of the incident by the entity, and not the actual **"occurrence"** of the incident [P 664].

CIP-008-2 and CIP-008-3 were silent regarding the required timeframe for reporting, but it was specifically addressed in CIP-008-5. In the October 26, 2012, redlined version of CIP-008-5, the proposed language for initial notification originally specified "one hour from **identification**" of an incident. This aligned with the Commission's decision in Order No. 706, for the clock to start with the discovery of an incident. However, the Standard Drafting Team changed "one hour from identification" to "one hour from the **determination** of a Reportable Cyber Security Incident". This language was subsequently approved and incorporated into CIP-008-5.

These changes, from "occurrence" to "discovery" to "determination," provide the additional time needed for the entity to apply its specifically created process(es) for determining whether a Cyber Security Incident rises to the level of required reporting. This determination timeframe may include a preliminary investigation of the incident which will provide useful information to other entities to help defend against similar attacks.

Notification Updates

Requirement R4 Part 4.3 requires that Responsible Entities submit updates for the required attributes upon determination of new or changed attribute information, if any. The SDT added this language to provide entities sufficient time to determine attribute information, which may be unknown at the time of initial notification, and which may change as more information is gathered. The intent of Requirement R4 Part 4.3 is to provide a method for Responsible Entities to report new information over time as their investigations progress. NOTE: The SDT does not

---

[2] 2008, Federal Energy Regulatory Commission, Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706.

intend updates specified in Requirement R4. Part 4.3 to expose responsible entities to potential violations if, for example, initial and updated notification on the same attribute have different information. This is expected since knowledge of attributes may change as investigations proceed. Rather, the intent of Requirement R4 Part 4.3 is to have a mechanism to report incident information to E-ISAC and NCCIC (and thereby industry) upon determination of each required attribute.

The intent is that the entity report what is known and document the reason not all attributes could become known and ultimately be reported in conditions where, e.g. a Cyber Asset was restored completely, removing all forensic evidence in order to restore operations, which caused the entity to conclude its investigation without having a complete knowledge of the three required attributes.

The SDT asserts that nothing included in the new reporting Requirement R4, precludes the entity from continuing to provide any voluntary sharing they may already be conducting today.

Technical Rationale for Reliability Standard CIP-008-5

This section contains the Guidelines and Technical basis as a "cut and paste" from CIP-008-5 standard to preserve any historical references.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for Reportable Cyber Security Incidents.

Entities may use an actual response to a Reportable Cyber Security Incident as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise.

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for Reportable Cyber Security Incidents. There are several examples of specific types of evidence listed in the measure.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

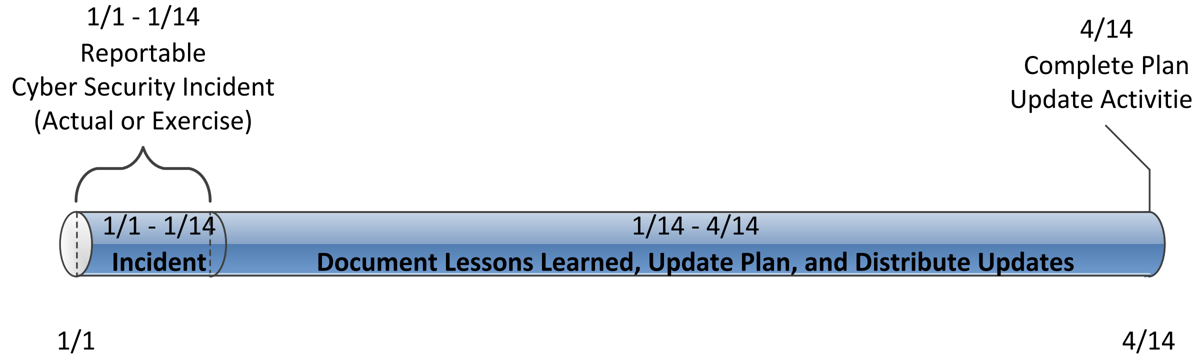
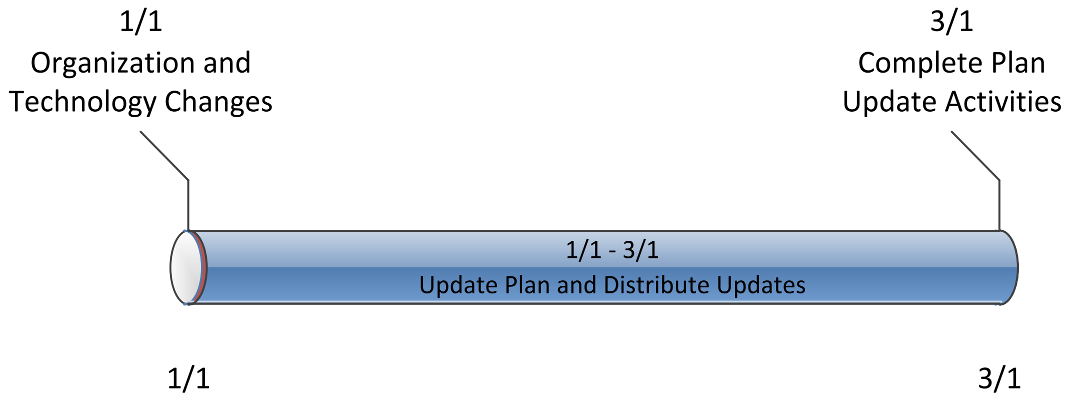


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in **Error! Reference source not found.**, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals.

Figure 2: Timeline for Plan Changes in 3.2



Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)
"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)
Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)
Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)
Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)
Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)
Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)
Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Exhibit E-8

CIP-009-7

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Recovery Plans for BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-009-7

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-009-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-009-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-009-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition Advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 – Requirement R3

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-009-7 to align recovery planning requirements with the virtualization changes and Shared Cyber Infrastructure (SCI).

The use of the term BES Cyber System has been replaced with “Applicable System” within the requirement language of Requirement R1 Part 1.3 and Requirement R2 Part 2.2 to align the requirement with the applicability for each Requirement Part.

Requirement R1 Part 1.5 has added ‘SCI supporting an Applicable System in this Part’ to the applicability. This requires that SCI be included in the process to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Having any SCI included in the forensics for a compromised applicable VCA, or the SCI itself, is the reason for the inclusion.

SCI is not specifically included in any other Requirement Parts of CIP-009, because CIP-009 focuses on the ability to recover the BCS functionality, which may or may not require recovery of SCI. The SDT has therefore not included SCI as a direct object of the other recovery plan Requirements and Parts. However, if recovery of the Applicable System’s functionality is dependent on recovery of any SCI, then the recovery plan(s) should include such dependencies.

Former Background Section from Reliability Standard CIP-009-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.

An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-009-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-009-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, “A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Tabletop exercises (TTX)] can be used to assess plans, policies, and procedures.”

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, “[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and ‘boots on the ground’ response (e.g., firefighters decontaminating mock victims).”

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

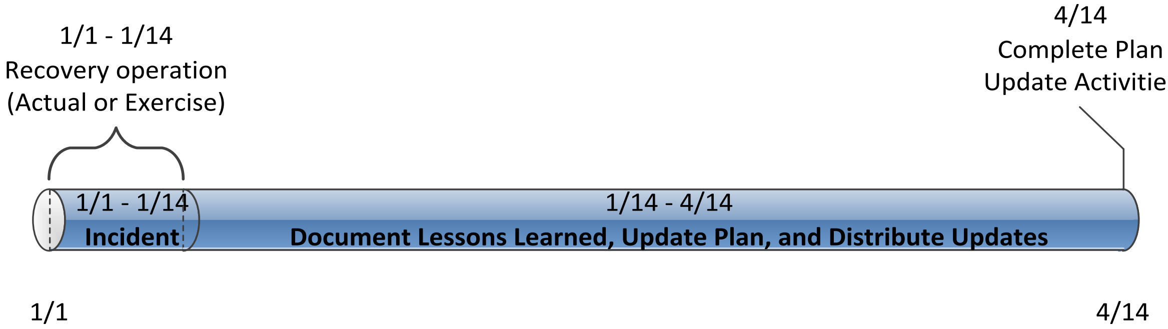


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

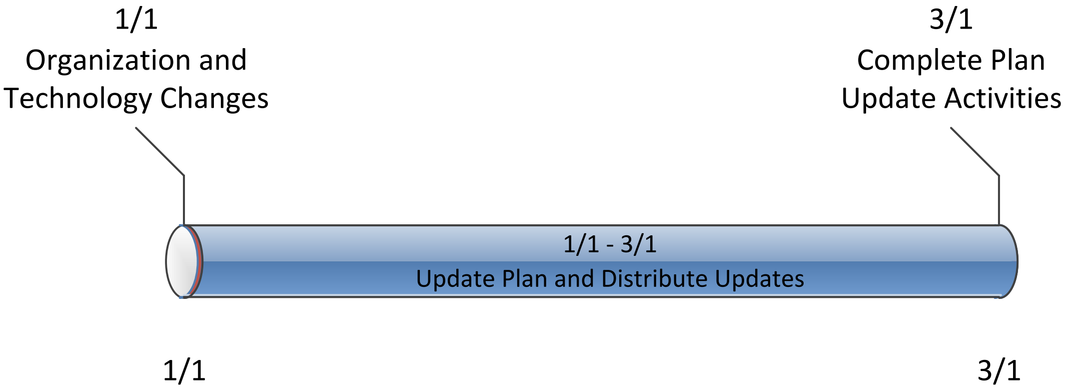


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Exhibit E-9

CIP-010-5

Cyber Security — Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-5

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-010-5

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-5. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-010-5 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference.

Virtualization Concepts Driving CIP-010 Changes

The proposed changes in CIP-010-5 from the Project 2016-02 SDT concern the use of several facets of virtualization technologies. Virtualization allows for such technologies as new controls for Shared Cyber Infrastructure (SCI), remediation VLAN, containers, parent/child images, and dormant virtual machines (VMs). Enabling and clarifying the use of these technologies is the basis of the proposed changes in CIP-010-5. A general introduction to each of these technologies follows.

Shared Cyber Infrastructure (SCI)

Where entries elect to utilize "Shared Cyber Infrastructure", virtualization abstracts the software layers (the OS and applications) from the underlying hardware to allow the hardware infrastructure to be shared among several Virtual Cyber Assets (VCAs) that may be of differing impact levels. Hypervisors must include security controls to keep these workloads logically isolated from one another and those requirements are within other CIP standards such as CIP-005 and CIP-007. However, with any type of shared infrastructure, the need for change management requirements is elevated for those security controls that allow for the 'shared' in SCI. Such controls are added to the change management requirements in CIP-010-5. As discussed elsewhere, entities may choose to high watermark all VCAs executing in their virtualized infrastructure, known as the "all-in" scenario, and not be concerned with SCI specific requirements. They simply consider the underlay part of the highest impact BCS executing on it and comply with the appropriate security controls and requirements for it.

Remediation VLAN

Remediation VLAN is a term used to describe a logical network segment in which a Cyber Asset or VCA can be isolated from having routable connectivity to any BES Cyber Systems (typically only having visibility of remediation services such as patching and antimalware updates, etc.) while it is examined to ensure the integrity and validity of the configuration and software installed on it. After this examination and subsequent remediation of deficiencies is completed, it is then joined to its production network.

This examination is policy driven, meaning that the administrator is able to configure what the minimum requirements are for a successful examination. Examples of this might be minimum operating system patch levels or recent anti-virus definitions.

If during the examination of the asset, it is found to not comply with the requirements defined in the policy, an administrator may intervene to manually remediate the deficiencies, or the system which was used to examine the asset may communicate the deficiencies to the asset with instructions on how to remediate itself in an automated fashion. After the remediation actions are taken, the asset can request to be re-examined and if the requirements dictated by the policy are now met, it will be joined to its production network.

Containers (Application Containers)

Containers are a form of virtualization at an individual application level, bundling the application code and its runtime environment into a self-contained, sandboxed environment. The application can then be instantiated dynamically on one or multiple dynamic hosts. The benefit is it makes the application or logic as portable as possible and able to be instantiated as-is without modification on a developer’s workstation, a test environment, or a production data center without the notion of installing the application or the various runtime dependencies into a particular OS instance. This notion of applications no longer being installed into an OS has significant implications for previous versions of CIP-010 R1 which were based almost solely on a ‘baseline configuration’ of installed software. The images from which application containers are instantiated that meet the conditions of R1.1 should not be outside the scope of change authorization because they are not “installed” in a particular instance of an OS. To limit R1 to only “installed” software may leave out the way applications are beginning to be delivered in systems of today.

Parent/Child Images

When a VCA is ‘powered on’ or begins execution, it instantiates (“boots”) from a disk image file. Since the boot ‘disk’ is a file and not physical disk, many individual VCAs can use the same “parent” image as the basis for their own “child” image. Among other things, this allows for patching of an OS to occur to a parent image and the child images then pick up that patched image upon their next instantiation. A common use of parent/child images is Virtual Desktop Infrastructures (VDI) that deliver a temporary desktop environment to each remote user for the duration of their session that are VCAs instantiated from a parent image.

Dormant VMs

A VCA that is not currently executing or instantiated (i.e., not ‘booted up’) is a dormant VM. It exists not as a traditional VCA, but simply as a file. VCA’s can be created for specialized purposes such as to run troubleshooting tools and are only instantiated when needed and may be dormant for long periods of time. They are not instantiated and on the network where they are managed and patched on a regular basis. However, these can go hand-in-hand with remediation VLANs which would bring them up to date as soon as they do begin to instantiate.

General Considerations

SCI is mutually exclusive from Cyber Assets (CA) by definition. To enable CIP-010-5 for virtualization, the SDT evaluated the existing Applicable Systems and added “SCI that supports an Applicable System in this Part”. This approach keeps the SCI applicability parallel to each existing variant of Medium Impact BCS (i.e. Medium Impact BCS vs. Medium Impact BCS with External Routable Connectivity (ERC) vs. Medium Impact BCS at Control Centers etc.).

Requirement R1

General Considerations for Requirement R1

In prior versions, CIP-010 Requirement R1 has required developing a baseline configuration that consisted of five (5) items (OS or firmware, installed and custom software, ports, and patches). The baseline configuration was then used in the remainder of Requirement R1 and R2 as the basis of change management including testing. At a high level, the CIP-010-4 Requirement Part 1.1 was to develop a baseline configuration, Requirement R1 Part 1.2 was to authorize and document changes to the items in the baseline configuration, and Requirement R1 Part 1.3 was to update the baseline configuration within a specific timeframe after a change. This tended to focus the requirement on maintaining documentation of past changes. However, in CIP-010-4 the core security objective of R1 was in Part 1.2 to authorize and document changes and the baseline configuration was used primarily to set the scope of those changes. Maintaining the baseline configuration information within 30 days after making changes is not a security objective, and as we implement more dynamic systems and more automation of change with virtualization, it becomes more problematic.

In CIP-010-5, the SDT considered the more dynamic, policy-based, and automated virtualization technologies discussed in the previous section and determined to focus Requirement R1 on the true security objective of change management and authorizing intended changes for those changes that can affect the security posture. In other words, make R1.2 from version 4 the main focal point in version 5. Maintaining documentation of ever more automated updates to systems after the fact gives way in this version to authorizing changes that will affect the security posture of the system. The SDT is addressing VCA’s that may be dormant for long periods of time and dynamically patched at a future instantiation when needed. The SDT considered the focus of R1 is not for entities to track the date/time a VCA may be dynamically instantiated and patched in an automated fashion in a remediation VLAN and then provide evidence that a baseline configuration was updated within 30 days of that dynamic event.

In addition, with the introduction of application containers and orchestration (Kubernetes, Docker Swarm, etc.), application software may no longer be “installed” on a particular OS instance on a particular server. Instead, an orchestration service may instantiate an application container on the best “node” (server with container runtime) at the moment. For example, a dedicated “database server” gives way to a “database service” that can be instantiated in a container on any VCA or CA managed by the orchestrator. Therefore, baseline configurations of statically installed software and open ports loses value as it becomes dynamically managed in these scenarios. The focus of R1 has thus changed from documenting the installed software and its open ports on a Cyber Asset or VCA at some point post-change to authorizing the changes that will occur to it when it does instantiate, which provides more security value.

Entities may of course continue to maintain and use baseline configurations, but in CIP-010-5 it is no longer the singular prescribed way of setting change management scope and documenting changes. Baseline configurations may continue to be used as evidence for CIP-007 R1 for example, documenting the enabled ports on a system. In fact, baseline configurations will probably continue to be a very common method used by entities to help detect unauthorized changes in CIP-010 R2, but the standard does not prescribe it as the singular way to meet these security objectives. Therefore, the phrase “baseline configuration” has been removed from CIP-010-5 though entities may continue using it as their “how”. Again, the focus of R1 in CIP-010-4 and CIP-010-5 is authorizing changes that affect the security posture of the applicable systems; the SDT has just brough it forward as the “what” with baseline configurations as one possible, but not prescribed, “how”. Entities may also wish to reference NIST SP 800-128 “Guide for Security-Focused Configuration Management of Information Systems” as a guide for additional information.

The SDT also considered at length the scope of changes that should be subject to R1. In CIP-010-4, the scope was set by the prescribed elements in the baseline config, consisting essentially of software, patches, and ports. As mentioned above, the security objective of putting ports in the baseline configuration is not to document and maintain a list of listening ports; that security objective is covered in CIP-007 R1 to reduce the attack surface by disabling unneeded ports. Maintaining documentation of the patches installed on a system (which becomes more problematic over time with vendor-bundled monthly updates that may install/remove patches differently per each system's needs) is not the security objective. Knowing what patches are available and applicable to the systems and installing them and mitigating the risk is the goal as covered in CIP-007 R2. In CIP-010 R1, authorizing the action in order to manage change is the objective.

In addition, the SDT considered the prescribed list of baseline configuration elements was insufficient as the scope of a change management requirement. For example, in an SCI that is configured to isolate VCAs of different impact levels from each other, managing and authorizing change to that configuration is vital. As Zero Trust architectures come to fruition, managing and authorizing changes to those access policies is crucial. These are all very important security configurations that were not enumerated in CIP-010-4's baseline configuration and thus not in scope. The SDT concluded that creating a longer prescriptive list of items was not appropriate, in that such a list would need to be maintained as technology changes. The SDT decided to put objective language in the requirement and use the Measures to show examples of more detailed lists of items.

Rationale for Requirement R1 Part 1.1

The SDT brought the security objective to the forefront in this requirement part by starting it with "Authorize changes…". Next it narrows the scope to those "that affect Applicable Systems" and the SDT made conforming changes to Applicable Systems to add SCI. The SDT considered that many entities scope their own internal change management processes this way; if a change is to or affects something in their NERC CIP program for medium/highs, it goes through change management. However, the requirement needs a bit more precise scoping accomplished with the objective language of "…altered behaviors…" to the underlying technical controls so it doesn't include changes such as a user changing their password or desktop background, or a system log being written to hundreds of times an hour. The requirement needs a lower bound, a floor, without attempting to incorporate a prescriptive list of change types or categories.

The SDT used the objective language "…where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 and CIP-007, as defined by the Responsible Entity." The intent is to bound the scope to those changes that affect the system's CIP security posture. *More precisely, the intent is to set the floor of the scope to changes that alter the behavior of a cyber security control the entity uses to keep the system secure per CIP-005 and CIP-007 requirements.*

The phrasing "alter the behavior of one or more cyber security controls" is intended to help clarify the scope. For example, the intent is that a user changing their password is not in scope; that is a change that may be required on some periodicity by a cyber security control such as a domain password policy but is not a change that alters the behavior *of the control itself*. What would be in scope is a change to that domain password policy.

The "excluding procedural and physical controls" (as well as the "*cyber security* controls" phrase) is intended to exclude from CIP-010 R1's scope changes to controls from CIP-005 and CIP-007 that are not technical controls. An example would be an entity may have signage or port-blockers as a procedural/physical control for meeting CIP-007 R1.2 concerning physical ports. Installing/removing port blockers or changes to the signage is not intended to be subject to CIP-010 R1. A change to the affinity rules for a hypervisor, if the entity uses that in an SCI scenario to meet CIP-007 R1.3, would meet the intent, as well as changes to EAP firewall rules/policy that the entity uses as the control to meet CIP-005 R1. The configuration of anti-malware controls the entity uses, such as update mechanisms or alerting mechanisms that change *how* the control functions in meeting CIP-007 R3 would be included but not the regular signature updates the control uses; those are not changes to the control's configuration that alter the way the control behaves.

Along these lines, rather than including a prescriptive list of change categories or types within the requirement, the SDT did analyze the requirements in CIP-005 and CIP-007 and included examples of cyber security controls that may serve those requirements in the Measures column to help clarify the intent. These are examples and are not a mandatory prescriptive list of the types of changes that would be included and for which evidence of authorization through change records could be provided.

It is important to note the SDT did not include prescriptive timeframes for this requirement. The rationale for this is to account for emergency changes, those that need to occur for reliability of the system when it may not be possible to put in a request and gain authorization beforehand. The SDT intent is for these system reliability related emergency changes to not become a violation of this standard, which it would if it had "prior to" type phrases within it, or required prescriptive definition of what constitutes emergency changes, etc. However, emergency changes will still need to be authorized, after the fact, to meet the requirement.

Rationale for Requirement R1 Part 1.2

Requirement R1 Part 1.2 is where CIP-010-4 Requirement R1 Part 1.5 now lands in CIP-010-5, with minor modifications to Part 1.2.1, and conforming changes to remove the 'baseline configuration' terminology to enable for virtualization.

The SDT chose to remove the reliance on a "Technical Feasibility Exception" in favor of permitting "CIP Exceptional Circumstances" in Part 1.2.1. The SDT contends testing in a test environment prior to implementing any change in production, and documenting test results may impede Responsible Entities' efforts to recover from events or conditions that qualify as CIP Exceptional Circumstances, and that term still requires an entity to document when that condition occurs with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception (TFE).

Additionally, Requirement R1 language negates the need for both the "technically feasible" and "per system capability" because the focus is on testing the implemented CIP-005 and/or CIP-007 cybersecurity controls the responsible entity determines as serving the requirements in CIP-005 and CIP-007 and require authorization. If a particular CIP-005 or CIP-007 cyber security control cannot be implemented due to "technical infeasibility" or "per system capability", then that unimplemented cyber security control would not be in scope for CIP-010-5 Requirement R1, nor Requirement Part 1.2 rendering the need for that language moot.

Additionally, the SDT chose to add to the phrase "that minimizes differences with the production environment" to eliminate the dependency on baseline configuration, as well as to mitigate the need for a TFE.

Rationale for Requirement R1 Part 1.3

Conforming changes to Applicable Systems (see General Considerations above).

Requirement R1 Part 1.3 is where CIP-010-4 Requirement R1 Part 1.6 now lands in CIP-010-5, with conforming changes to remove the 'baseline configuration' terminology and instead referring to operating systems, firmware, software, or software patches changes as the trigger for the Requirement Part.

The SDT acknowledges virtualization vendors may provide a "golden image" to clone multiple other Virtual Cyber Assets as described in the "Parent/Child Images" section above. The SDT intent is for entities that use the golden image technology to account for the software source and integrity of the golden image which covers any unmodified clones derived from it.

Rationale for Requirement R1 Part 1.4

Requirement Part 1.4 is a simplified version of the same part 1.4 in the previous version. The SDT made conforming changes to align the scope of this part with 1.1 with the phrasing "As a part of the changes authorized per Part 1.1…".

It is important to note the SDT intent and rationale behind the wording "As a part of the change". The rationale for that phrase is the entity, before closing out that change, will verify that the change has not adversely affected the altered cyber security controls. If the entity, as part of the post change verification, finds that it did, the entity must remediate that issue. The intent is this change not be completed until it is verified that the cyber security controls are not adversely affected.

What was 1.4.1 in the previous version required the entity to determine, prior to the change, the CIP-005 and CIP-007 controls that might be affected. With the automated remediation technology at instantiation, this is no longer possible and the SDT considered it was not the security objective. The security objective, the required behavior, is that entities ensure that changes don't adversely affect the cyber security controls by verifying them after making the change. That is now the clearly stated focus of 1.4. It is not the SDT's intent that the entity must test *every* cyber security control for *every* change, which is the rationale for the wording "of the altered cyber security controls". If an entity is installing a patch to an application on a BCS, it's not the intent that the entity verify that the domain password policy wasn't changed, however, the entity should verify the patch did not open or enable any unnecessary ports for example. The requirement part 1.4.3 from the previous version to document the results of the verification has been deleted and the SDT rationale is that is essentially a requirement to provide evidence for the actions taken to comply with the requirement part. Therefore 1.4 is now a simplified security objective to be met.

The rationale for the phrasing of "adversely affected" is simply to recognize that the desired effect of a change may be to impact a cyber security control – for example an entity may wish to change a password policy such that it requires stronger passwords than the CIP standard requires. That would not be an "adverse" change.

Requirement R2

General Considerations for Requirement R2

The scoping of Requirement R2 is an intentional subset of the scope for Requirement R1. The focus of CIP-010-5 Requirement R1 is authorizing changes that affect the security posture of those Applicable Systems as well as the logical environments that protect them. This is why R1 includes the obligation to authorize changes that alter the behavior of one or more cyber security controls that are implemented to protect the system or environment. The Applicable Systems for the R2 monitoring requirement for unauthorized changes is an intentional a subset of cyber security controls (CIP-007) to align with the Appliable Systems scope and those technical controls that have been implemented at the System or Cyber Asset level to maintain that cyber security posture.

The SDT has reworked R2 for monitoring for unauthorized changes to work better with the additional scope of R1's change management. The SDT's rationale is that all changes that should be included and authorized in a change management program may not have an automated solution for monitoring for unauthorized change and the SDT's intent is for this requirement's scope to be items that have a greater potential to for automated monitoring by technical controls, recognizing monitoring outputs (alarms, alerts, reports, logs etc.) may require manual review by the recipients to determine if the change was unauthorized and what subsequent actions, if any, may need to be taken. Therefore, the SDT tied R2 loosely to R1's scope but with a required list of seven cyber security-related categories to monitor. The SDT's intent when using the 'per system capability' language is to keep the scope of R2 to those things for which automated solutions are available and likely to monitor these areas and alert entities to changes. It should be noted the 'system' in 'per system capability' refers to the Applicable Systems for the requirement, and not the capability of the automated tool used to monitor. As a result, the 'per system capability' language does not absolve entities of the obligation to implement monitoring methods where automated solutions have not been implemented, and while potentially less ideal, manual methods to accomplish the same results where automated monitoring cannot be done remains a requirement where the Applicable System is capable of producing data related to the list of seven cyber security-related categories to monitor. The reference to manual reviews is also in the measures because the manual response actions to automated monitoring serves as supporting evidence and a means to demonstrate compliance with the final component of Part 2.1, which is to 'Document and investigate detected unauthorized changes'.

The SDT has added the term "unauthorized" into Requirement R2 Part 2.1 to focus it on the risk of unauthorized changes. Many implementations will perform this task by monitoring all changes and looking for unauthorized changes within that population. However, the SDT is allowing for a capability that may filter out authorized changes such that the entity can have methods to monitor for unauthorized changes only. The SDT also added "per system capability" in recognition that not all changes in scope can be monitored on every potential in-scope Cyber System.

This addition makes the requirement conditional if a system is incapable of monitoring a particular unauthorized change category.

The SDT has used the phrasing “that include at least one cyber security control for each of the following” in order to allow entities to monitor a primary security control if they have multiple overlapping controls. The SDT’s intent is that having multiple security controls over these categories is a good and beneficial practice where possible, and entities should not be discouraged from having more than one. This phrasing’s intent is to allow the entity to choose the primary control they monitor for unauthorized change. The entity may of course do more than one, but one is required.

For the seven required control categories, the SDT notes it intent as follows:

2.1.1 – The intent is to monitor for changes to the system’s configuration affecting ports or services that are enabled such that they provide accessibility via routable protocols on a network interface.

2.1.2 – The SDT notes that the intent of this item is conditional – evidence for this is only required “on SCI”. If there is no SCI, then no control is required. If SCI is in scope, then some control to monitor for unauthorized changes to CPU/memory sharing of VCAs (affinity rules, etc.) is required.

2.1.3 - The intent of this is the traditional monitoring of changes to executable code of the various listed types. As noted in the Measures column, the SDT intends to handle the parent/child image issues by monitoring the parent image from which temporary child images are derived. See the “Parent/Child Images” section earlier in this document for examples.

2.1.4 – The intent is to monitor for unauthorized changes to the configuration of malicious code protection methods, for example whether they have been disabled, or alerting turned off, etc. Note this is not the detection or alerting or remediation of malicious code that is covered in CIP-007; this is monitoring the configuration of your method to ensure its configured behavior has not been changed in an unauthorized manner.

2.1.5 – Similar to 2.1.4, this is not monitoring the security event log and alerting as covered in CIP-007; this is monitoring the configuration of your security event logging and alerting for unauthorized changes that would change its expected behavior (disabling it, changing what is logged, changing where alerts go, etc.)

2.1.6 – The intent of “configuration of authentication methods” is to monitor for configuration changes that affect how a system authenticates its users/processes. Examples would include password policies (not individual user passwords), configuration of multi-factor authentication, changes to Pluggable Authentication Modules (PAM) on Linux systems, etc.

2.1.7 – Along with 2.1.6 concerning how a system is configured to authenticate users, this requires a control to monitor for unauthorized changes to enabled or disabled status of accounts. For example, if a “Guest” account or a default “admin” account have been disabled on a system, monitoring for the unauthorized re-enabling of those accounts.

Requirement R3

Rationale for Requirement R3 Part 3.1

Conforming changes only to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.2

Conforming changes to Applicable Systems (see General Considerations above).

The SDT chose to remove the reliance on a “Technical Feasibility Exception” in favor of the updated term “per system capability”. The SDT contends that the term still requires an entity to document the limit to the system’s

capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

In Requirement R3 Part 3.2.1, conforming changes have been made to remove the baseline configuration dependency. Additionally, the SDT chose to add to the phrase "that minimizes differences with the production environment" to eliminate the dependency on baseline configuration.

Rationale for Requirement R3 Part 3.3

The previous language of "Prior to adding a new applicable Cyber Asset to a production environment" for the timing of performing a vulnerability assessment has an interesting "chicken or egg" problem when it comes to VCAs. This phrasing for the timing has worked well for hardware "programmable electronic devices" arriving on a loading dock or spares coming in from a warehouse that should be assessed before being physically placed "in production". However, VCA's aren't shipped, they are created in the production environment from a hardware perspective. A VCA image may be created on the hypervisor, an OS installed, the appropriate applications installed, etc., but the VCA is not yet connected to its production network and instantiated in a way that it has connectivity or is performing its function. However, it is from a hardware standpoint in the "production environment" so you can't do an assessment "prior to" that as this is where it's created.

To solve this issue, the SDT replaced this timing phrasing with the language "Prior to becoming a new Applicable System…". The SDT's rationale is the requirement part requires the vulnerability assessment at a point prior to the VCA being instantiated, with the "production" connectivity it requires, to perform its function either as a part of a BES Cyber System or EACMS or PCA. As it begins to perform those functions (i.e., for an EACMS to begin controlling or monitoring electronic access), it becomes an "Applicable System" at that point – prior to that point in time the vulnerability assessment of that VCA should have taken place. The remediation VLAN technologies may perform this automatically at every instantiation. The SDT made this change so that the requirement part did not imply that VCAs had to be created elsewhere, in some other separate hardware environment, assessed, and then somehow imported. Conforming changes have been made to remove the baseline configuration dependency. The exceptions are "Like replacements or additions with a previously assessed configuration of an existing Applicable System; or CIP Exceptional Circumstances".

Conforming changes made to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.4

Conforming changes made only to Applicable Systems (see General Considerations above).

Requirement R4

General Considerations for Requirement R4

The SDT updated Requirement R4 to include associated SCI into the scope of the required plans for Transient Cyber Assets (TCA) and Removable Media. The SDT also updated Attachment 1, such that the scope is clarified once within Requirement R4 and applies throughout Attachment 1.

The SDT corrected a perceived mismatch of control to objective by moving the control "Live operating system and software executable only from read only media;" from Part 1.3 to Part 1.4 as a better location for the control to serve the objective of the Part, which aligns with Sections 2.1 & 2.2.

The SDT also made several conforming changes to Attachment 1 for TCAs to ensure continuity in language between the measures and similar sections in CIP-003 Attachment 1.

Former Background Section from Reliability Standard CIP-010-4

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.
Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-010-4

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

---

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

---

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management. With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity’s responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity’s security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity’s plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rationale for Reliability Standard CIP-010-3

This section contains a “cut and paste” of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset’s baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset’s baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity’s use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to “model” the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media.

The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit E-10

CIP-011-4

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Information Protection

Technical Rationale and Justification for Reliability Standard CIP-011-4

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-011-4

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-011-4 . It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-011-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

General Considerations

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-011-4 to align information protection requirements with the virtualization changes.

Requirement R1 and R2

Rationale

To enable CIP-011-4 for virtualization, the SDT added "Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part" within the Applicable Systems column of each of the Parts for Requirement R1 – Requirement R2.

Requirement R2 Part 2.1

Requirement R2 Part 2.1 is an objective level requirement focused on protecting BES Cyber System Information (BCSI) rather than 'Cyber Assets' and 'storage media' and was modified to include the currently approved Requirement R2 Part 2.2. This consolidation is necessary to enable flexibility, allowing for cryptographic erasure in scenarios where BCSI cannot be mapped to one or more disks within a virtualized storage cluster, and where BCSI is stored on Cyber Systems employing deduplication. This adjustment is also future-looking to better position CIP-011 for the enablement of cloud type scenarios where the disks are owned and/or managed by a third-party as a service to the entity for its BCSI storage, analysis, or use.

Requirement R2 Part 2.2

Requirement R2 Part 2.2 has been deleted because it was consolidated into Requirement R2 Part 2.1.

Former Background Section from Reliability Standard CIP-011-3

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-011-3

Requirement R1

General Considerations for Requirement R1
None

Rationale for Modifications to Requirement R1:
Requirement R1 still specifies the need to implement one or more documented information protection program(s). The SDT does not intend that this requirement cover publicly available information, such as vendor manuals or information that is deemed to be publicly releasable. Information protection pertains to both digital and hardcopy information.

The SDT clarified the intent of protecting BCSI as opposed to protecting the BES Cyber System(s) and associated applicable systems which may contain BCSI. This was achieved by modifying the parent CIP-011-X R1 requirement language to include "for BES Cyber System Information (BCSI) pertaining to Applicable Systems".

Rationale for Modifications to Requirement R1, Part 1.1
Requirement R1, Part 1.1, is an objective level requirement focused on identifying BES Cyber System Information (BCSI). The intent of the SDT was to simplify the requirement language from CIP-011-2 Part 1.1.

Rationale for Modifications to Requirement R1, Part 1.2
Requirement R1, Part 1.2, is an objective level requirement focused on protecting and securely handling BES Cyber System Information (BCSI) in order to mitigate risks of compromising confidentiality. The reference to different states of information such as "transit" or "storage" or "use" was removed. The intent is to reduce confusion of Responsible Entities attempting to interpret controls specific to different states of information, limiting controls to said states, overlapping controls between states, and reduce confusion from an enforcement perspective. By removing this language, methods to protect BCSI becomes explicitly comprehensive.

Requirement language revisions reflect consistency with other CIP requirements.

Requirement R2

General Considerations for Requirement R2
None

Rationale for Requirement R2:
The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BCSI upon reuse or disposal.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement 2 has remained unchanged. The requirements are focused more on the reuse and disposal of BCS rather than BCSI. While acknowledging that such BCS and other applicable systems may have BCSI residing on them, the original intent of the requirement is broader than addressing BCSI. This is a lifecycle issue concerning the applicable systems. CIP-002 focuses on the beginning of the BCS lifecycle but not an end. The potential end of the applicable systems lifecycle is absent from CIP-011 to reduce confusion with reuse and disposal of BCSI. The 2019 BCSI Access Management project did not include modification of CIP-002 in the scope of the SAR. This concern has been communicated for future evaluation.

Technical Rationale for Reliability Standard CIP-011-2

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-011-2 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].

Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit E-11

CIP-013-3

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-3

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-013-3

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-3. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-013-3 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-013-3 to align supply chain risk management requirements with the virtualization changes.

To enable CIP-013-3 for virtualization, the SDT added "and Shared Cyber Infrastructure (SCI)" to the parent Requirement R1. Additionally, the SDT simplified the applicability in Requirement R1 Parts 1.1 and 1.2 by replacing the long list of applicable systems with a reference to the list in the parent Requirement R1 through the use of this language, "applicable systems listed in Requirement R1". Note: Because CIP-013-3 does not contain the "Table" construct with an "Applicable Systems" column, this term is not defined within Section 4 Applicability; Therefore, where used, "applicable systems" is intentionally not capitalized within the requirement language of Requirement R1 Parts 1.1 and 1.2.

Technical Rationale for Reliability Standard CIP-013-2

This section contains a “cut and paste” of the Technical Rationale for CIP-013-2 standard to preserve any historical references.

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team’s (SDT’s) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission’s Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17,

2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

---

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however, chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

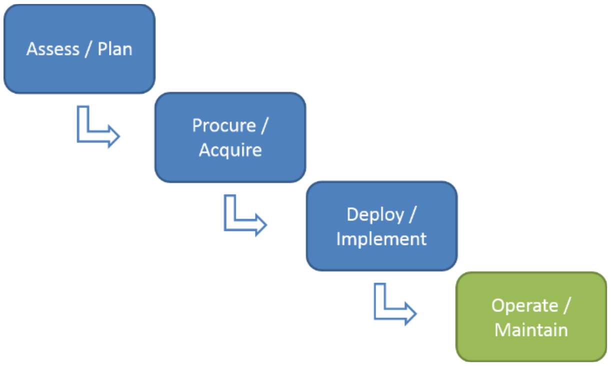
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R3

General Considerations for Requirement R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

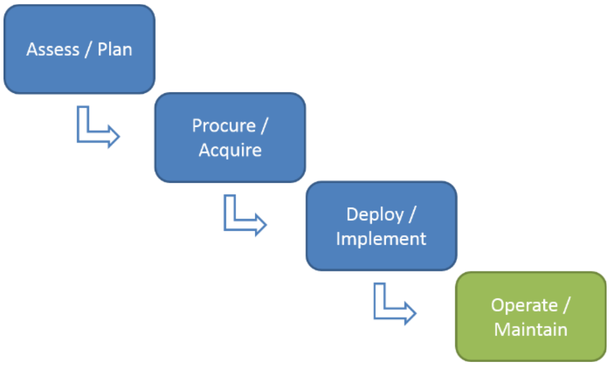
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit E-12

Definitions and Exemptions

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Technical Rationale

New and Modified Terms, and Exemption Language Used in NERC Reliability Standards | Project 2016-02 Modifications to CIP Standards

Introduction

The standard drafting team (SDT) has in several terms made changes based on the intent that the glossary is a dictionary and defines what something is, not its security requirements or necessarily the scope of systems those requirements apply to. The rationale for such changes is:

- If scoping of which specific systems is included in the definition, the definition can no longer be used in other standards or other requirements with a differing scope. If what the term defines is needed in a differing requirement of a slightly different scope, either the definition must change affecting all uses of it in all standards, or we proliferate more glossary terms to include differing scopes in the definition. Removing specific scoping in definitions alleviates this concern. Several terms below now use a far more generic 'Cyber System' in the definition with the specific scoping of requirements left to those requirements in the standards.
- If implicit requirements are included in the definition (e.g., such as where in relation to an Electronic Security Perimeter (ESP) an Intermediate System must be implemented), then if an entity implements that one aspect incorrectly, that is non-conformant with a glossary term, the unintended consequence is that it may lead to non-compliance with all requirements that rely on that term. Putting any requirement-type language in requirements rather than definitions alleviates this concern.

Proposed Modified Terms:

BES Cyber Asset (BCA)

A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the Reliable Operation of the Bulk Electric System (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Rationale

The BCA definition was modified to allow for BCA to be either Cyber Assets (hardware included) or Virtual Cyber Assets (VCA) (software only virtual machines without the underlying hardware). See the VCA and Shared Cyber Infrastructure (SCI) definition below. Note that SCI is not included because if the hardware is supporting VCAs of differing impact levels, it is not a BCA with a single impact category, but it is SCI and subject to the additional "SCI only" requirements. If all the hosted VCAs are treated as "associated PCAs" of the highest impact BCS, then the underlying hardware is no longer SCI and is a BCA of the same impact rating as the highest impact BCS it hosts. The SDT also capitalized the term “Reliable Operation” to tie this to “instability, uncontrolled separation, and cascading” as that is a defined term in the NERC Glossary providing more clarity. Additionally, the glossary term uses the Bulk Power System scope, but the BCA definition uses the specific scope “Reliable Operation of the Bulk Electric System” just as the Reliability Coordinator definition does.

BES Cyber System Information (BCSI)

Information about the BES Cyber System (BCS) that could be used to gain unauthorized access or pose a security threat to the BCS. BCSI does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BCS, such as, but not limited to, device names, individual IP addresses without context, Electronic Security Perimeter names, or policy statements. Examples of BCSI may include, but are not limited to, security procedures or security information about BCS, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BCS.

Rationale

The BCSI definition was modified with conforming changes such that BCSI examples include information about SCI that could be used to gain unauthorized access or pose a security threat to the BCS.

Critical Infrastructure Protection (CIP) Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Cyber Security Standards.

Rationale

The CIP Senior Manager definition was modified by removing explicit reference to the CIP standards as only “CIP-002 through CIP-011” since the body of CIP Cyber Security Standards has grown beyond CIP-011. For example, the CIP Senior Manager also has requirements within CIP-013.

Cyber Assets

Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCA) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.

Rationale

The Cyber Asset definition was modified to explicitly exclude SCI from the definition of Cyber Asset such that SCI is a different hardware class on which the other VCAs of differing impact levels execute. SCI is defined separately such that it can be the object of additional requirements based on its unique risks. The definition is also modified to clarify that ‘Application containers’ (i.e., portable, packaged applications) are considered software of a Cyber Asset (or VCA), though they may have some characteristics of a VCA (a container can be instantiated with its own IP address, etc.). This is because of their packaged quality, typically being updated as a whole and not as individual components, and the limited capabilities that containers have. When viewing applications containers as something to apply CIP Requirements to, the concept breaks down quickly due to the nature of container platforms. Additionally, the capabilities that containers do possess, that would offer services on a network for example, would then exist on the VCA or Cyber Asset that the container is running on and can be controlled as part of the required set of controls for that device. Additionally, executing instances of VCAs are not to be considered simply software or data of the Cyber Asset.

Cyber Security Incident

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System (BCS), compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System, or (4) Shared Cyber Infrastructure; or
- Disrupts or attempts to disrupt the operation of a BCS.

Rationale

The Cyber Security Incident definition was modified to add SCI to the scope of compromised or attempted compromises of, the listed perimeters and systems.

Electronic Access Control or Monitoring Systems (EACMS)

Cyber System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) (ESP) or BES Cyber Systems (BCS), including those not protected by an ESP used by the Responsible Entity to convert routable protocol communications to non-routable communications to a BCS.

Rationale

The EACMS definition was modified to add Cyber Systems so that VCA and SCI are included as two other forms that an EACMS can take. Removed the explicit inclusion of Intermediate Systems as that was moved to the Intermediate Systems definition. Added the inclusion of certain protocol conversion scenarios where the protocol converter is clarified to be an EACMS. This involves a Cyber Asset that does perform electronic access control or monitoring that is also converting from a routable protocol (e.g., IP over Ethernet) to non-routable protocol (e.g., ASCII text over serial) to BCS that are themselves non-routable (serial) only. The SDT intent is this does not include “bump in the wire” type converters (i.e., IP to serial converters) that have no capability to identify users and perform electronic access control or monitoring. It does include those Cyber Assets that users login and select a serial port to then communicate with a BCS and are clearly performing electronic access control or monitoring. In this latter scenario, though the BCS itself is serial non-routable only and therefore has no ESP, the converter is still performing as an EACMS. It may also be performing as an Intermediate System for IRA to the serial only BCS (see changes to the IRA definition).

Electronic Access Point (EAP)

An electronic policy enforcement point or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.

Rationale

As network security moves deeper into the infrastructure, it’s no longer necessary to prescribe that network security be performed only at a ‘Cyber Asset interface on an ESP’ at one point on a network edge. Zero Trust, for example, highly distributes the network security model and is not perimeter-based, and this is incorporated through the addition of “electronic policy enforcement point or”. With the added flexibility in CIP-005 to adopt these models in addition to the traditional ESP model, the EAP definition was modified to allow for electronic policy enforcement points and no longer prescribes an architecture. The “one or more” and the “associated PCAs” have been added to clarify that EAPs can control communications to a group and not required per individual system.

External Routable Connectivity (ERC)

The ability to access a BES Cyber System through its Electronic Security Perimeter via a bi-directional routable protocol connection.

Rationale

The ERC definition was modified to allow for zero trust or other network models that are not strictly perimeter or network-border based, thus not having concepts of “inside” or “outside”. These concepts are replaced with the language “through its ESP” so that it does not imply a prescriptive network security model. The ERC term is used throughout the CIP Standards within the Applicable Systems column as a scoping mechanism based on the inherent risk associated with ERC as well as to limit the scope of requirements that would require ERC to function. The SDT is maintaining this use of ERC, but also clarifying the relationship between ERC and Interactive Remote Access (IRA) in that a non-routable, serial only BCS (thus with no ESP) may have IRA through a subsequent IP/serial conversion (see changes to IRA definition).

Electronic Security Perimeter (ESP)

The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points.

Rationale

The ESP definition was modified to provide flexibility and the use of various architectures and access control models. The traditional network border ESP remains a valid network security model, however it is no longer the only prescribed model as CIP-005 allows other access control models that are not based on network perimeters such as Zero Trust architectures. The proposed ESP definition retains its current definition but appends “or a logical boundary defined by one or more EAPs” to incorporate models that move away from implicit trust within network perimeters and using network location as a primary factor in access control decisions. In these models, the perimeter shrinks to increasingly more granular levels, potentially down to a process or resource level on a BCS. The proposed definition allows for an ESP to be (a) a border surrounding an isolated network that has no external connectivity and thus no EAPs, (b) static point(s) on a network boundary such as a traditional firewall as an EAP that is enforcing access policies or configurations (e.g., firewall rulesets), (c) many dynamic, short-lived, session-level ‘perimeters’ established at time of access that are network independent (e.g., users to resources, for example), or (d) hybrid implementations combining elements of more than one model.

The SDT has kept the ‘logical border’ concept for the “surrounding a network” ESP and used the language “logical boundary” for zero trust models. A ‘border’ does indeed surround an object, in this case a network, but a ‘boundary’ may not surround or enclose, it’s a line that can be crossed, such as a policy enforcement point controlling access to a resource. The SDT has also updated language in the standards to remove concepts such as ‘inside’ an ESP and replaced that with more inclusive phrases such as ‘protected by’ an ESP.

Interactive Remote Access (IRA)

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Entity’s Electronic Security Perimeter(s) (ESP);
- That is converted by the Responsible Entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

- Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs;
- System-to-system process communication.

Rationale

The IRA definition was modified in two fundamental ways: (1) to incorporate IRA situations where users outside of any of the Responsible Entity’s ESPs have interactive access, using a routable protocol, to a non-routable (e.g., serial) Cyber System through a subsequent IP to serial conversion, and (2) to include Management Interfaces as targets of IRA. Note that the scope of which Cyber Systems and Management Interfaces is contained within the applicable requirements in the standards and are not in the definition. The philosophy is scoping of requirements should be in the requirements to keep the definitions usable in other requirements with a different scope if needed. The references to ownership of the remote client have been removed as they are immaterial to the definition of IRA.

The definition begins with “User-initiated electronic access by a person using a bi-directional routable protocol” to match the human interactive (bi-directional) nature of the access to the requirements that secure such access in CIP-005 R2. For example, a batch process cannot read a multi-factor token and enter its displayed code; that security control is designed for interactive humans initiating a remote access session. Also note the person is using a routable protocol to initiate the access.

The definition outlines three targets of IRA:

1) "To a Cyber System protected by an Entity's Electronic Security Perimeter(s) (ESP)" covers the typical Cyber System that is connected to a network via a routable protocol and thus is protected by an ESP. In this instance, the remote user is using a routable protocol and is accessing a Cyber System on a routable protocol network, for example in a typical LAN-WAN-LAN, end to end routable protocol communication.
2) "That is converted by the Responsible Entity to a non-routable protocol that allows access to a Cyber System" clarifies IRA scenarios where the user is using a routable protocol to a site where the Responsible Entity then connects that session (e.g., using a gateway or terminal server) to a device's non-routable serial port to provide interactive remote access to the user. A common example is connecting a serial port on a digital relay in a substation to a terminal server or gateway device which is then connected to a routable network in the substation for the purpose of granting a remote user interactive access to the relay without traveling to the substation. This 2nd target of the definition now clarifies this is IRA even though the device itself may not have an ESP if it is only connected serially.

   Note the clarification and explanation in the EACMS definition above that applies to this scenario. The phrase "converted *by the Responsible Entity*" clarifies certain situations that may involve more than one entity and is best described by an example. Entity 1 has a BCS in a substation or generating resource that Entity 2, a Control Center, needs to access. Entity 2 provides a circuit to Entity 1's site and provides Entity 1 with a serial cable to connect to their BCS. This phrase clarifies that Entity 1 does not require detailed architectural knowledge of what Entity 2 does upstream with the data once delivered to the serial interface if Entity 1 does not do any conversion to routable protocols. If Entity 2 does convert to routable protocols and does provide IRA, then Entity 2 implements the IRA security controls on their routable protocol portion.
3) "To a Management Interface" adds the Management Interface as a valid target of IRA. Note the scope of Management Interfaces covered by CIP is in the CIP-005 requirements, not in the definition.

The definition then has two exclusions of scenarios that are not IRA:

1) "Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs" carries forward this exclusion from the previous definition and is intended to exclude, for example, the scenario of a Control Center operator within one of the Responsible Entity's ESPs interacting with field devices within its other ESPs, because for it to meet the IRA definition, IRA must originate from somewhere other than one of the Responsible Entity's protected ESPs.
2) "System-to-system process communication" carries forward this exclusion from the previous definition to clarify that a process that cannot for instance perform multi-factor authentication using tokens or biometrics is not IRA. It is instead covered by CIP-005 R1.

Note that the definition uses the more generic term Cyber Systems. This is in keeping with using the glossary as a dictionary that merely defines a term, in this case a type of access, but does not create or scope CIP requirements within the definition. The scope is in CIP-005 R2's requirement language. The intent is to create definitions that are scope agnostic so they can be used in multiple standards or requirements with varying scope in each.

Intermediate Systems

One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.

Rationale

The Intermediate System definition was modified by removing embedded requirement language (i.e., where an Intermediate System must reside). That language moved to CIP-005 Requirement R2 within a mandatory requirement. The definition was also updated from a Cyber Asset focus to an EACMS focus to include other forms (i.e., VCA) the Intermediate System may take. This also moves the clarification of "This includes Intermediate Systems" out of the EACMS definition into this one.

Physical Access Control Systems (PACS)

Cyber Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.

Rationale

The PACS definition was modified to use the term Cyber Systems to add VCA and SCI as two other forms that a PACS can take.

Physical Security Perimeter (PSP)

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Rationale

The PSP definition was modified to add SCI as type of Cyber System to be included within a PSP.

Protected Cyber Asset (PCA)

One or more Cyber Assets or Virtual Cyber Assets (VCA) that:

- Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or
- Share CPU resources or memory resources with any part of the BCS, excluding VCAs that are being actively remediated in an environment that isolates routable connectivity from BCS;

Excluding Transient Cyber Assets.

Rationale

The PCA definition was modified to ensure additional implementation scenarios in a virtualized environment that present similar risks to the BCS are accounted for through PCA protections. The PCA definition exists to identify other Cyber Assets or VCAs that must be protected by various CIP requirements due to what they share with a BES Cyber System. This sharing could allow the PCA to be a 'pivot point', a location from which to access the BCS. In the past, this sharing was limited to local network connectivity; the PCA being a network peer within the same ESP. With virtualization there is now another aspect of sharing and the PCA definition was modified to include "share CPU resources or memory resources with any part of the BCS" to mitigate the risks of hardware-based vulnerabilities (e.g., Spectre, Meltdown, Rowhammer, Zenbleed, etc.) on SCI. Since virtualization can allow systems of differing trust levels to simultaneously execute on the same hypervisor servers in the hardware underlay and thus share the same CPU resources or memory resources, this addition to the PCA definition requires that those VCAs that do share CPU resources or memory resources with a BCS become associated PCA's of the BCS. This provides the high water marking of VCAs sharing a single hypervisor's CPU resources or memory resources. Affinity rules can be used within the virtualization configuration to prevent this situation and keep other VCAs of differing impact levels from becoming associated PCAs. Thus, there is no "mixed mode" allowed on the same CPU resources or memory resources.

Finally, the definition was modified to account for "remediation VLAN" automation of security controls where a VCA may instantiate in a logical network reserved for vulnerability assessment and updates (e.g., OS patches, AV updates, etc.) that limits its connectivity to only remediation resources during the remediation process. Even though it may share CPU resources or memory resources during the remediation, the intent is to exclude the VCA from becoming a PCA while temporarily in this state as its being updated prior to being connected to its production network.

Removable Media

Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure (SCI), (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, SCI, a network protected by an Electronic Security Perimeter, or a Protected Cyber Asset.

Rationale

The Removable Media definition was modified to add SCI as a target of the Removable Media connection and incorporate the new ESP definition ("protected by" rather than "within").

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BCS;
- An Electronic Access Control or Monitoring System of a high or medium impact BCS; or

- Shared Cyber Infrastructure supporting a BCS.

Rationale

The Reportable Cyber security Incident definition was modified to add compromised or disrupted SCI supporting a BCS as a target.

Transient Cyber Asset (TCA)

A Cyber Asset or Virtual Cyber Asset (VCA) that is:

1. Capable of transmitting or transferring executable code,
2. Not included in a BCS,
3. Not a Protected Cyber Asset (PCA) associated with high or medium impact BCS, and
4. Connected for 30 consecutive calendar days or less:
   - On a network within an Electronic Security Perimeter containing high or medium impact BCS; or
   - Directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a:
     - BES Cyber Asset;
     - Shared Cyber Infrastructure; or
     - PCA associated with high or medium impact BCS.

Virtual machines hosted on a physical Transient Cyber Asset (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Rationale

The TCA definition was modified to add VCA as a form a TCA can take. The SDT is addressing two different transient connection scenarios.

The first scenario is a physical TCA such as a laptop. These TCAs may require older, 32-bit software and OS to connect to and configure older equipment in the field. These are often executed within VM 'player' environments on the physical TCA. The SDT asserts these packaged environments in an image file on a physical TCA should not be considered their own distinct virtual TCA and included the statement "Virtual machines hosted on a physical TCA are treated as software on that physical TCA" within the definition. The SDT asserts that a user that is authorized to use the physical TCA should not be required to be separately authorized to execute the software they need to use on the TCA, simply because it's in an image file and executed in a VM "player" type environment on the TCA. The SDT also asserts that if the user 'checks out' a physical laptop TCA to perform a task, it should not be a standard violation if they do not also 'check out' any VM images residing on that physical TCA's disk. The intent is that physical TCA is considered a 'unit' to perform a job and not several distinct TCAs on one laptop.

The second scenario is a more recent phenomenon where a service vendor (e.g., a pen-tester or security firm) may send an entity a VCA image (e.g., a vulnerability scanner instance) to temporarily instantiate within their virtualization environment. This VCA may only exist for a few hours and is functionally no different than the vendor bringing a physical laptop and connecting it to a physical network switch to perform the same task as a TCA. This transient VCA is not a part of the entity's CIP program and is treated as a TCA. This also handles VCAs the entity creates for typical TCA uses but are normally dormant on the same hardware as the BCS (e.g., a VCA with Wireshark for troubleshooting network issues within a virtualized infrastructure).

Additionally, SCI was added as a target to which TCAs can be directly connected.

Proposed New Terms:

Cyber System

One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.

Rationale

The term Cyber System was defined to simplify applicability when referring in the standards or other definitions to all the forms an object may take (Cyber Asset, VCA, or SCI). If other forms are needed in the future, their addition to this one definition can reduce needed edits throughout the standards and definitions where it is used.

Management Interface

An administrative interface that:

- Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure;
- Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or
- Configures an EAP.

Rationale

The term Management Interface was defined so that requirements are established for SCI and EACMS Management Interfaces to target the unique risks for virtualized environments presented by unrestricted access to the Management Interfaces for such environments. With ‘infrastructure as a service’ (IaaS) environments, the management consoles can not only be used to create, but also to destroy or reconfigure virtual servers, networks, switches, firewalls, etc. The term also includes interfaces commonly known as ILO (Integrated Lights Out), that can be used to remotely access the console. It also includes interfaces used to configure an EAP (such as on firewalls or a network switch that is enforcing an ESP between different virtual networks (e.g., VLANs). Note that scoping is included in requirements in the standard, not in the definition.

Shared Cyber Infrastructure (SCI)

One or more programmable electronic devices, including the software that shares the devices’ resources, that:

- Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber System (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control

Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or

- Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also, for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.

SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.

Rationale

The term SCI was defined to separate the underlying hardware from VCAs in the situation where the shared hardware resources support VCAs of varying impact levels. This allows security requirements to be targeted to SCI to address the unique risks of shared hardware. There are many requirements that now include the newly defined term SCI in the "Applicable Systems" column to maintain security level parity with traditional Cyber Assets.

Beyond security level parity with protecting a typical hardware based Cyber Asset, the SCI can have a more significant impact in a virtualized environment since it can host, and therefore impact, multiple virtualized systems of varying impact levels. Because of this capability, some additional controls only apply to SCI, such as the management plane isolation required by the proposed CIP-005. Addressing these unique risks requires separation of the hardware underlay into a separate definition.

The phrase "SCI does not include the supported VCAs or Cyber Assets with which it shares its resources" is included to clarify that, for example, electronic access to a hosted VCA by a user is not electronic access to the SCI on which it executes.

Of note is that shared network devices are not in the scope of this definition. Since network switches and firewalls share their resources by nature, this exclusion avoids pulling all network hardware into scope as SCI. However, network switches and other hardware that does enforce an ESP, such as a network switch configured to host different VLANs to which systems of differing impact levels are connected, comes into scope as an EACMS.

Virtual Cyber Asset (VCA)

A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset, Electronic Access Control or Monitoring System, Physical Access Control System, Protected Cyber Asset, or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include:

- Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems;
- Dormant file-based images that contain operating systems or firmware; and
- SCI or Cyber Assets that host VCAs.

Application containers are considered software of VCAs or Cyber Assets.

Rationale

The term VCA was defined to allow the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined as is the case in the Cyber Asset definition. The NERC Glossary definition of Cyber Asset has a direct tie to its hardware and software ("including the hardware, software, and data in the device") and assumes the electronic device is self-contained with a one-to-one relationship between a device and its software (including the operating system). This affected the definitions of the "Applicable Systems" terms such as BCS, EACMS, PACS, and PCAs that were all based on the Cyber Asset definition. Because the Reliability Standard is applicable to the aforementioned systems, the security controls for the Cyber Assets also applies to the hardware. The one-to-one relationship between a Cyber Asset and its underlying hardware and software is what virtualization intentionally breaks to increase reliability and resiliency by allowing VCAs to be abstracted from the hardware and therefore able move to any available hardware out of a pool of resources.

The phrase "currently executing on a virtual machine" is used to clarify:

- That a VCA does not include disk image files that are not currently instantiated or executing and are thus providing no functions or services.
- That a "logical instance of an operating system or firmware" only refers to those running on a hypervisor as a virtual machine and does not refer to a locally installed OS or firmware on the hardware.

The definition excludes "logical instances that are being actively remediated…" to allow for automated solutions (such as remediation VLANs) to bring newly instantiated instances into compliance in an isolated environment before they are moved to production networks and begin providing their function or service, at which point they become a VCA.

The phrase "hosted on a BCA, EACMS, PACS, PCA, or SCI" is to clarify that an entity for an "all-in" scenario can still classify the underlying hardware as one or several of these types, yet the VCAs remain their own object subject to requirements and are not simply "software in the device" as in the Cyber Asset definition.

Examples of VCAs may include, but are not limited to, logical instances of the following:

- Operating Systems (Virtual Machines (VM));
- Networking devices such as switches, routers, and load balancers;
- Security appliances such as firewalls and VPN concentrators; and
- Helper appliances with logical connectivity (such as malware detection, plugins, etc.).

The definition also clarifies that 'Application containers' (i.e., portable, packaged applications) are considered software of a VCA or Cyber Asset, though they may have some characteristics of a VCA. This is because of their packaged quality, typically being updated as a whole and not as individual components, and the limited capabilities that containers have. When viewing applications containers as something to apply CIP Requirements to, the concept breaks down quickly due to the nature of container platforms. Additionally, the capabilities that containers do possess, that would offer services on a network for example, would then exist on the VCA or Cyber Asset that the container is running on and can be controlled as part of the required set of controls for that device.

Technical Rationale for Exemptions Section:

Rationale for Exemption 4.2.3.1

The term 'Cyber Assets' was replaced with the new proposed term 'Cyber Systems'. Rather than changing this language to a list of all possible forms (Cyber Assets, VCAs, or SCI) as the object of the exemption, the SDT chose to instead use the existing language in the 4.2.3.4 and 4.2.3.5 exemptions such that all five exemptions use a form of 'systems' as their object.

Rationale for Exemption 4.2.3.2 and 4.2.3.3

In 4.2.3.2, the term 'Cyber Assets' was replaced with the new proposed term 'Cyber Systems' which is a new proposed glossary addition. Rather than changing these two exemptions to list all possible forms (Cyber Assets, VCAs, or SCI), the SDT chose to define a new term that incorporates all forms and use it within the multiple exemptions and at other points within the standards.

For 4.2.3.3, the ability to move workloads or VMs seamlessly across different sites for increased resiliency can require different sites to be connected as a flat network without layer 3 ESPs at each discrete site (e.g., a layer 2 adjacency across the sites). A "Super ESP" as it has been historically known is created across the sites and thus an exemption based on having a discrete layer 3 ESP at each site no longer works to exclude, for example, the network transport equipment that may belong to carriers. The SDT included the 4.2.3.3 exemption to further clarify this scenario. Responsible Entities should notice the exemption uses the word "between" – when extending an ESP between geographic locations, CIP-005 requires the confidentiality and integrity protection of the data (typically through encryption) between the relevant PSPs. This exemption then covers the related Cyber Systems "between" those encryption points but does not exclude the endpoints performing the encryption.

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit F

Analysis of Violation Risk Factors and Violation Severity Levels

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in the project-related standards. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

The VRFs and VSLs can be found within each Reliability Standard. This document provides justification for Reliability Standards with more substantive changes to the VRFs and VSLs, not justification for the Reliability Standards without substantive changes or only conforming changes to VRFs and VSLs from the last FERC-approved versions.

- CIP-002-7: There were no changes to VRFs and only conforming or non-substantive changes to VSLs.
- CIP-003-10: There were no changes to VRFs and justification for VSLs is provided below.
- CIP-004-8: There were no changes to VRFs and justification for VSLs is provided below.
- CIP-005-8: There were no changes to VRFs and justification for VSLs is provided below.
- CIP-006-7: There were no changes to VRFs and only conforming changes to VSLs.
- CIP-007-7: There were no changes to VRFs and justification for VSLs is provided below.
- CIP-008-7: There were no changes to VRFs and no substantive changes to VSLs.
- CIP-010-5: There were no changes to VRFs and justification for VSLs is provided below.
- CIP-011-4: There were no changes to VRFs and no substantive changes to VSLs.
- CIP-013-3: There were no changes to VRFs and no substantive changes to VSLs.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management

- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VSL justification for CIP-003-10 Requirements R1, R2, R3, and R4

The VSLs were revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-003-10, Requirements R1, R2, R3, and R4	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-004-8 Requirement R1

The VSL did not substantively change from the previously FERC approved Reliability Standard CIP-004-7.

VSL justification for CIP-004-8 Requirements R2, R3, R5 and R6

The VSLs were revised for readability by deleting the deliverable language associated with certain violations.

VSL justification for CIP-004-8 Requirement R4

The VSLs were revised from the previously FERC approved Reliability Standard CIP-004-7 to add a moderate VSL and a high VSL to account for failing to authorize electronic access based on need for one or two individuals, respectively, to be consistent with the VSL in Requirement R5 and to align with FERC VSL G2a.

VSL Justifications for CIP-004-8, Requirements R2, R3, R4, R5 and R6	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-004-8, Requirements R2, R3, R4, R5 and R6	
Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-005-8 Requirement R1

The VSL changed from the previously FERC approved Reliability Standard CIP-005-7:

1. To add severe VSLs to conform with the addition of SCI to Appliable Systems;
2. To accommodate for the modified requirement part language to enable for virtualization through protections for Management Interfaces, routable protocol communications, and the exclusion time sensitive communications of Protection Systems;
3. To account for the consolidation of the previously FERC approved CIP-006-6 Requirement R1 Part 1.10 into the final draft of CIP-005-8 Requirement R1 Part 1.6; and
4. Were also revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-005-8, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-005-8, Requirement R1	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-005-8 Requirement R2

The VSL changed from the previously FERC approved Reliability Standard CIP-005-7.

1. To add severe VSLs to conform with the addition of SCI to Appliable Systems;
2. To accommodate for the modified requirement part language to prevent Intermediate Systems from sharing CPU resources or memory resources with any part of a high or medium impact BCS, and to ensure routable protocol communications from and Intermediate System to a high or medium BCS went through an ESP; and
3. Were revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-005-8, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-005-8, Requirement R2	
for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-005-8 Requirement R3

The VSL changed from the previously FERC approved Reliability Standard CIP-005-7:

1. To add severe VSLs to conform with the addition of SCI to Appliable Systems; and
2. Were also revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-005-8, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity

VSL Justifications for CIP-005-8, Requirement R3	
Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-007-7 Requirement R1

The VSL changed from the previously FERC approved Reliability Standard CIP-007-6:

1. To add lower and high VSLs to align with FERC VSL G2a;
2. To accommodate for the modified requirement part language to prevent sharing of CPU resources or memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS;
3. To account for network accessible services; and
4. Were revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-007-7 Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-007-7 Requirement R1	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-007-7 Requirement R2
The VSLs were revised for readability by deleting the deliverable language associated with certain violations and to assure consistency in language by qualifying the term ‘patches’ with ‘cyber security’.

VSL justification for CIP-007-7 Requirements R3 and R4
The VSLs were revised for readability by deleting the deliverable language associated with certain violations.

VSL justification for CIP-007-7 Requirement R5
The VSLs were revised for readability by deleting the deliverable language associated with certain violations and updated to accommodate for the replacement of technical feasibility exception language with per cyber system capability language in certain requirement parts.

VSL Justifications for CIP-007-7 Requirements R2, R3, R4 and R5	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-007-7 Requirements R2, R3, R4 and R5	
Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-010-5 Requirement R1

The VSL changed from the previously FERC approved Reliability Standard CIP-010-4:

1. To add moderate VSLs to conform with the addition of SCI to Appliable Systems; and
2. To accommodate for the consolidated requirement parts and language to enable for virtualization through the shift from a prescriptive baseline to an objective level requirement for processes to authorize changes that alter the behavior of cyber security controls serving the requirement parts of CIP-005 and CIP-007.

VSL Justifications for CIP-010-5 Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-010-5 Requirement R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-010-5 Requirement R2

The VSL changed from the previously FERC approved Reliability Standard CIP-010-4 to align with FERC VSL G2a:

1. By adding a moderate, and a high VSL to account for failing to include in documented and implemented configuration monitoring process(es) ‘one or two’, or ‘three or four’, of the required Parts 2.1.1 through 2.1.7 for Applicable Systems, respectively; and modifying the severe VSL for failing to include 5 or more of the required Parts 2.1.1 through 2.1.7 for Applicable Systems in documented and implemented configuration monitoring process(es).
2. By adding a lower, moderate, and a high VSL to account for failing to monitor within 35 calendar days and exceeding the required cadence by monitoring for 36 to 69 calendar days, 70 to 104 calendar days, 105 to 139 calendar days, respectively; and modifying the severe VSL for failing to monitor for 140 calendar days or more as required by Part 2.1.

VSL Justifications for CIP-010-5 Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-010-5 Requirement R2	
for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-010-5 Requirements R3 and R4

The VSLs were revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-010-5 Requirements R3 and R4	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-010-5 Requirements R3 and R4	
Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

Exhibit G

Summary of Development History and Complete Record of Development

Summary of Development History

The following is a summary of the development record for proposed Reliability Standards. As development of the proposed Reliability Standards occurred over several years, the versions of the proposed Reliability Standards shifted if other versions of the same Reliability Standard were developed concurrently. As such, the complete record of development provides those shifts in version numbers, while the summary of development maintains the version numbers proposed in the petition.

I. Overview of the Standard Drafting Team

When evaluating a proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[1] The technical expertise of the ERO is derived from the drafting team ("DT") selected to lead each project in accordance with Section 4.3 of the NERC Standard Processes Manual.[2] For this project, the DT consisted of industry experts, all with a diverse set of experiences. A roster of the Project 2016-02 – Modifications to CIP Standards DT members is included in **Exhibit H**.

II. Standard Development History

A. Standard Authorization Request Development

On March 9, 2016, the Standards Committee authorized posting a Standards Authorization Request ("SAR") to address Commission directives from Order No. 822[3] and CIP Version 5 Transition Advisory Group issues for a 30-day informal comment period from March 23, 2016 through April 4, 2016 and authorized solicitation of nominations for the Project 2016-02 –

---

[1] Section 215(d)(2) of the Federal Power Act; 16 U.S.C. § 824(d)(2) (2022).

[2] The NERC *Standard Processes Manual* is available at https://www.nerc.com/AboutNERC/RulesOfProcedure/Appendix_3A_SPM_Clean_Mar2019.pdf.

[3] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, at P 17, *order on reh'g,* Order No. 822-A, 156 FERC ¶ 61,052 (2016).

Modifications to CIP Standards DT.[4] Based on comments received, the DT revised the SAR and posted for another 30-day informal comment period from June 1, 2016 through June 30, 2016. The Standards Committee accepted the revised SAR on July 20, 2016.[5]

B. First Posting - Comment Period, Initial Ballot, and Non-binding Poll

On January 20, 2021, the Standards Committee authorized initial posting of the proposed Reliability Standards and associated definitions, the associated Implementation Plan, Violation Risk Factors ("VRFs"), Violation Severity Levels ("VSLs"), and other associated documents for a 60-day formal comment period from January 22 – March 22, 2021, with a parallel initial ballot and non-binding poll held during the last 10 days of the comment period from March 12 – March 22, 2021.[6] There were 91 sets of responses, including comments from approximately 210 different individuals and approximately 133 companies, representing all 10 industry segments.[7] The following table provides for each Reliability Standard: 1) the percentage of affirmative votes,[8] 2) the quorum reached, and 3) the results of the non-binding poll and quorum for the associated VRFs and VSLs.

Standard	Approval	Quorum	Non-binding Poll / Quorum
CIP-002-7	38.97	91.42	43.46 / 90.61
CIP-003-10	48.44	91.09	53.72 / 90.25
CIP-004-8	51.31	91.03	61.17 / 90.25
CIP-005-8	26.36	91.03	29.32 / 89.53
CIP-006-7	42.81	91.03	48.37 / 89.21
CIP-007-7	42.43	91.03	48.17 / 89.21
CIP-008-7	52.87	91.03	62.84 / 89.21

---

[4] NERC, *Meeting Minutes – Standards Committee Meeting Mar. 9, 2016.*

[5] NERC, *Meeting Minutes – Standards Committee Meeting July 20, 2016.*

[6] NERC, *Minutes – Standards Committee Meeting Jan. 20, 2021*, Agenda Item 6, https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_January_Minutes_Approved_February_17_2021.pdf.

[7] NERC, *Consideration of Comments – Virtualization*, *Project 2016-02 Modifications to CIP Standards July 2021,* https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016-02_CIP_Virtualization_Consideration_of_Comments_for_Draft_1_072021.pdf.

[8] A ballot needs 66 and two-thirds percentage approval to pass.

CIP-009-7	53.26	90.7	62.64 / 88.85
CIP-010-5	32.53	91.03	38.74 / 89.21
CIP-011-4	47.38	90.7	59.89 / 89.21
CIP-013-3	51.37	90.7	59.78 / 89.21

C. Second Posting - Comment Period, Additional Ballot, and Non-binding Poll

The proposed Reliability Standards and associated definitions, the associated Implementation Plan, VRFs, VSLs, and other associated documents were posted for a 64-day formal comment period from June 30 – September 1, 2021, with a parallel additional ballot and non-binding poll held during the last 10 days of the comment period from August 23 – September 1, 2021. There were 93 sets of responses, including comments from approximately 218 different individuals and approximately 137 companies, representing all 10 industry segments.[9] The following table provides for each Reliability Standard: 1) the percentage of affirmative votes, 2) the quorum reached, and 3) the results of the non-binding poll and quorum for the associated VRFs and VSLs.

Standard	Approval	Quorum	Non-binding Poll/Quorum
CIP-002-7	36.32	88.12	37.36 / 87.73
CIP-003-10	41.67	88.12	43.96 / 88.09
CIP-004-8	38.21	88.37	44.81 / 88.09
CIP-005-8	20.31	88.04	19.67 / 88.09
CIP-006-7	42.32	88.04	45.6 / 88.13
CIP-007-7	29.49	88.04	28.02 / 87.77
CIP-008-7	49.63	88.37	52.46 / 88.13
CIP-009-7	49.88	88.37	53.3 / 87.77
CIP-010-5	33.32	88.37	36.07 / 88.13
CIP-011-4	40.29	88.37	45 / 87.73
CIP-013-3	41.56	88.37	45.56 / 87.41

---

[9] NERC, *Draft 2 Consideration of Comments – Virtualization*, *Project 2016-02 Modifications to CIP Standards Feb. 2022*, https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016-02_Draft_2_Consideration_of_Comments_02182022.pdf.

D. Third Posting - Comment Period, Initial Ballot, and Non-binding Poll

The proposed Reliability Standards and associated definitions, the associated Implementation Plan, VRFs, VSLs, and other associated documents were posted for a 54-day formal comment period from February 18 – April 12, 2022, with a parallel additional ballot and non-binding poll held during the last 12 days of the comment period from April 1 – April 12, 2022. There were 85 sets of responses, including comments from approximately 187 different individuals and approximately 125 companies, representing all 10 industry segments.[10] The following table provides for each Reliability Standard: 1) the percentage of affirmative votes, 2) the quorum reached, and 3) the results of the non-binding poll and quorum for the associated VRFs and VSLs.

Standard	Approval	Quorum	Non-binding Poll/Quorum
CIP-002-7	72.84	82.89	80 / 81.25
CIP-003-10	73.36	82.89	77.25 / 81.25
CIP-004-8	76.97	83.11	79.64 / 81.25
CIP-005-8	60.73	83.11	63.41 / 81.25
CIP-006-7	76.08	83.11	82.63 / 80.95
CIP-007-7	61.36	83.11	65.06 / 80.95
CIP-008-7	78.62	83.11	83.23 / 80.95
CIP-009-7	78.37	82.77	82.63 / 80.95
CIP-010-5	56.69	82.77	66.46 / 80.95
CIP-011-4	79.04	82.77	82.53 / 80.95
CIP-013-3	78.62	83.11	82.42 / 80.95

E. Fourth Posting - Comment Period, Additional Ballot, and Non-binding Poll

The proposed Reliability Standards and associated definitions, the associated Implementation Plan, VRFs, VSLs, and other associated documents were posted for a 52-day formal comment period from August 17 – October 7, 2022, with a parallel additional ballot held during the last 10 days of the comment period from September 28 – October 7, 2022 and non-

---

[10] NERC, *Draft 3 Consideration of Comments – Virtualization*, *Project 2016-02 Modifications to CIP Standards Aug. 2022,* https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016-02_Virtualization_Draft_3_Consideration_of_Comments_08312022.pdf.

binding poll held from September 28 – October 10, 2022. There were 72 sets of responses, including comments from approximately 188 different individuals and approximately 121 companies, representing all 10 industry segments.[11] The following table provides for each Reliability Standard: 1) the percentage of affirmative votes, 2) the quorum reached, and 3) the results of the non-binding poll and quorum for the associated VRFs and VSLs.

Standard	Approval	Quorum	Non-binding Poll/Quorum
CIP-002-7	94.63	77.89	97.25 / 80.87
CIP-003-10	84.90	77.89	87.36 / 76.09
CIP-004-8	84.60	78.07	88.46 / 80.87
CIP-005-8	65.26	78.41	69.95 / 81.23
CIP-006-7	92.60	78.07	93.44 / 80.58
CIP-007-7	67.38	77.74	73.08 / 80.58
CIP-008-7	95.67	77.74	96.7 / 80.58
CIP-009-7	95.38	77.74	96.15 / 80.58
CIP-010-5	46.35	78.07	57.46 / 80.58
CIP-011-4	82.59	77.74	87.5 / 80.94
CIP-013-3	82.88	77.74	87.98 / 80.58

F. Waiver

On October 19, 2022, the Standards Committee approved a waiver under Section 16.0 of the Standard Processes Manual authorizing additional formal comment and ballot periods to be

---

[11] NERC, *Draft 4 Consideration of Comments – Virtualization*, *Project 2016-02 Modifications to CIP Standards October. 2023*, https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016-02_CIP_Virtualization_Draft_4_Consideration_of_Comments.pdf.

reduced from 45 days to as few as 20 calendar days, with ballot conducted during the last 10 days of the comment period.[12]

G. Fifth Posting - Comment Period, Additional Ballot, and Non-binding Poll

In the fifth posting, the DT balloted those Reliability Standards that either did not achieve the requisite approval in the fourth posting or had further substantive revisions. The proposed Reliability Standards and associated definitions, the associated Implementation Plan, VRFs, VSLs, and other associated documents were posted for a 58-day formal comment period from October 3 – November 29, 2023, with a parallel additional ballot and non-binding poll held during the last 10 days of the comment period from November 20 – November 29, 2023. There were 71 sets of responses, including comments from approximately 185 different individuals and approximately 116 companies, representing all 10 industry segments.[13] The following table provides for each Reliability Standard: 1) the percentage of affirmative votes, 2) the quorum reached, and 3) the results of the non-binding poll and quorum for the associated VRFs and VSLs.

Standard	Approval	Quorum	Non-binding Poll/Quorum
CIP-003-10	93.80	83.5	92.61 / 82.29
CIP-004-8	84.73	84.41	81.03 / 83.03
CIP-005-8	72.73	84.41	70.18 / 83.03
CIP-007-7	89.32	84.41	87.79 / 82.35
CIP-010-5	74.46	84.75	75.14 / 83.09

---

[12] NERC, *Minutes – Standards Committee Meeting Oct. 19, 2022*, Agenda Item 6, https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC%20October%20Minutes%20-%20Approved%20December%2013,%202022.pdf.

[13] NERC, *Draft 5 Consideration of Comments – Virtualization*, *Project 2016-02 Modifications to CIP Standards April 2024*, https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20DL/2016-02_Consideration_of_Comments_04032024.pdf.

H. Final Ballot

The proposed Reliability Standards and associated definitions, the associated Implementation Plan, VRFs, VSLs, and other associated documents were posted for a 10-day final ballot from April 3 – April 12, 2024. The following table provides for each Reliability Standard: 1) the percentage of affirmative votes, and 2) the quorum reached.

Standard	Approval	Quorum
CIP-002-7	94.37	84.62
CIP-003-10	93.63	85.86
CIP-004-8	86.3	86.1
CIP-005-8	75.73	86.1
CIP-006-7	94.7	83.84
CIP-007-7	90.24	86.1
CIP-008-7	96.05	83.84
CIP-009-7	95.8	83.84
CIP-010-5	76.98	86.44
CIP-011-4	86.21	83.84
CIP-013-3	86.47	83.84

I. Board of Trustees Adoption

The NERC Board of Trustees adopted the Reliability Standards and associated definitions on May 9, 2024.[14]

---

[14] NERC, *Board of Trustees Agenda Package*, Agenda Item 5a (Project 2016-02 Modifications to CIP Standards) available at https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board%20of%20Trustees%20Agenda%20Package%20-%20May%209%202024.pdf.

Home > Program Areas & Departments > Standards > Project 2016-02 Modifications to CIP Standards

Project 2016-02 Modifications to CIP Standards

Related Files

Status

The final ballots for the **CIP Virtualization standards (outlined below)** concluded **8 p.m. Eastern, Friday, April 12, 2024**. The voting results can be accessed via the links below. The standards will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

-CIP-002-7 - Cyber Security – BES Cyber System Categorization

-CIP-003-10* - Cyber Security – Security Management Controls

-CIP-004-8* - Cyber Security – Personnel & Training

-CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation

-CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems

-CIP-007-7 - Cyber Security – Systems Security Management

-CIP-008-7 - Cyber Security – Incident Reporting and Response Planning

-CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems

-CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments

-CIP-011-4* - Cyber Security – Information Protection

-CIP-013-3 - Cyber Security – Supply Chain Risk Management

***Based on recent board adopted standards for CIP-003-9, CIP-004-7, and CIP-011-3, the posted versions for the 2016-02 Modifications to CIP Standards were updated to reflect CIP-003-10, CIP-004-8, and CIP-011-4. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-9, CIP-004-7, and CIP-011-3, the version numbers within this posting are correct and entities will be voting on CIP-003-10, CIP-004-8, and CIP-011-4.*

Background

The Version 5 Transition Advisory Group (V5 TAG) transferred issues to the Version 5 SDT that were identified during the industry transition to implementation of the Version 5 CIP Standards. Specifically, the issues that the SDT will address are:

- Cyber Asset and BES Cyber Asset Definition
- Network and Externally Accessible Devices
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations
- Virtualization

On January 21, 2016, FERC issued Order No. 822 Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC approved revisions to version 5 of the CIP standards and also directed that NERC address each of the Order 822 directives by developing modifications to requirements in CIP standards and the definition of Low Impact External Routable Connectivity (LERC), or the SDT shall develop an equally efficient and effective alternative. To address concerns identified in Order 822, the Commission directed the following:

- Develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability.
- Develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact).
- Develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule, to the LERC definition consistent with the commentary in the Guidelines and Technical Basis section of CIP-003-6.

Standard(s) Affected –CIP-002, CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, CIP-011, CIP-012-1, CIP-013

Purpose/Industry Need

The SDT will modify the CIP family of standards (or develop an equally efficient and effective alternative) to:

- Address issues identified by the CIP V5 TAG;
- Address FERC directives contained in Order 822; and
- Address requests for interpretations as directed by the NERC Standards

Subscribe to this project's observer mailing list

Select "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft **ZIP file to all documents** CIP-004-8 is the only standard with a redline to last posted included as it shows minor clarifying edits made by the team. The remaining standards had no edits made from the last posted version to this final ballot version so they are not included CIP-002-7 **(384)** Clean | **(385)** Redline to Withdrawn Version 6 | **(386)** Redline to Last Approved Version 5.1a CIP-003-10 **(387)** Clean| **(388)** Redline to Last Approved	Final Ballots **(435)**Info Vote	04/03/24 - 04/12/24	Ballot Results **(436)** CIP-002-7 **(437)** CIP-003-10 **(438)** CIP-004-8 **(439)** CIP-005-8 **(440)** CIP-006-7 **(441)** CIP-007-7	

CIP-004-8 **(389)** Clean | **(390)** Redline to Last Posted| **(391)** Redline to Last Approved CIP-005-8 **(392)** Clean | **(393)** Redline to Last Approved CIP-006-7 **(394)** Clean | **(395)** Redline to Last Approved CIP-007-7 **(396)** Clean | **(397)** Redline to Last Approved CIP-008-7 **(398)** Clean | **(399)** Redline to Last Approved CIP-009-7 **(400)** Clean | **(401)** Redline to Last Approved CIP-010-5 **(402)** Clean | **(403)** Redline to Last Approved CIP-011-4 **(404)** Clean | **(405)** Redline to Last Approved CIP-013-3 **(406)** Clean | **(407)** Redline to Last Approved **(408)** Implementation Plan Proposed New, Modified, and Retired Definitions Used in The Reliability Standards **(409)** Clean | **(410)**Redline **Supporting Materials** Technical Rationales **(411)** Definitions and Exemptions **(412)** CIP-002-7 **(413)** CIP-003-10 **(414)** CIP-004-8 **(415)** CIP-005-8 **(416)** CIP-006-7 **(417)** CIP-007-7 **(418)** CIP-008-7 **(419)** CIP-009-7 **(420)** CIP-010-5 **(421)** CIP-011-4 **(422)**CIP-013-3 **(423)** VRF/VSL Justifications RSAWs **(424)** CIP-002-7 **(425)** CIP-003-10 **(426)** CIP-004-8 **(427)** CIP-005-8 **(428)** CIP-006-7 **(429)** CIP-007-7 **(430)** CIP-008-7 **(431)** CIP-009-7 **(432)** CIP-010-5 **(433)** CIP-011-4 **(434)** CIP-013-3			**(442)** CIP-008-7 **(443)** CIP-009-7 **(444)** CIP-010-5 **(445)** CIP-011-4 **(446)** CIP-013-3	
Draft 5 CIP-003-10 **UPDATED 10/16/2023** **(340)** Clean | **(341)** Redline to Draft 4 Clean | **(342)** Redline to Last Posted | **(343)** Redline to Last Approved	Additional Ballots and Non-		Ballot Results **(374)** CIP-003-10 **(375)** CIP-004-8	

CIP-004-8 **(344)** Clean | **(345)** Redline to Last Posted | **(346)** Redline to Last Approved CIP-005-8 **(347)** Clean |**(348)** Redline to Last Posted | **(349)** Redline to Last Approved CIP-007-7 **(350)** Clean | **(351)** Redline to Last Posted | **(352)** Redline to Last Approved CIP-010-5 **UPDATED 10/16/2023** **(353)** Clean | **(354)** Redline to Draft 4 Clean | **(355)** Redline to Last Posted | **(356)** Redline to Last Approved Implementation Plan **(357)** Clean | **(358)** Redline Proposed New, Modified, and Retired Definitions Used in The Reliability Standards **(359)** Clean | **(360)** Redline **Associated Materials** **(361)** Unofficial Comment Form (Word) Technical Rationales **(362)** CIP-003-10 **(363)** CIP-004-8 **(364)** CIP-005-8 **(365)** CIP-007-7 **(366)** CIP-010-5	binding Polls **(371)** Ballot Open Reminder **(372)** Info **UPDATED** **(373)** Info Vote	11/20/23 - 11/29/23 **UPDATED**	**(376)** CIP-005-8 **(377)** CIP-007-7 **(378)** CIP-010-5 Non-binding Poll Results **(379)** CIP-003-10 **(380)** CIP-004-8 **(381)** CIP-005-8 **(382)** CIP-007-7 **(383)** CIP-010-5	
	Comment Period **(367)** Info**UPDATED** **(368)** Info Submit Comments	10/03/23 - 11/29/23 **EXTENDED**	**(369)** Comments Received	**(370)** Consideration of Comments
(338) Waiver **(339)** Meeting Minutes	The Standards Committee accepted the waiver on October 19, 2022			
Draft 4 CIP-002-7 **(263)**Clean | **(264)** Redline to Last Posted **(265)** Redline to Last Approved CIP-003-Y **(266)** Clean | **(267)** Redline to Last Posted | **(268)** Redline to Last Approved CIP-004-8 **(269)** Clean | **(270)** Redline to Last Posted |**(271)** Redline to Last Approved CIP-005-8 **(272)** Clean | **(273)** Redline to Last Posted **(274)** Redline to Last Approved CIP-006-7 **(275)** Clean | **(276)** Redline to Last Posted| **(277)** Redline to Last Approved CIP-007-7 **(278)** Clean | **(279)** Redline to Last Posted| **(280)** Redline to Last Approved CIP-008-7 **(281)** Clean | **(282** Redline to Last Posted | **(283)** Redline to Last Approved CIP-009-7 **(284)** Clean | **(285)** Redline to Last Posted | **(286)** Redline to Last Approved CIP-010-5 **(287)** Clean | **(288)** Redline to Last Posted| **(289)** Redline to Last Approved CIP-011-4 **(290)** Clean | **(291)** Redline to Last Posted | **(292)** Redline to Last Approved CIP-013-3 **(293)** Clean | **(294)** Redline to Last Posted| **(295)** Redline to Last Approved **(296)** Implementation Plan **(297)** Proposed New, Modified, and Retired Definitions Used in The Reliability Standards **Associated Materials** **(298)** Unofficial Comment Form (Word) Technical Rationales **(299)** Definitions and Exemptions **(300)** CIP-002-7 **(301)** CIP-003-Y	Additional Ballots and Non-ballot Pools **(311)** Updated Info (Ballots Open Reminder) **(312)** Info (Updated) Vote	09/28/22 - 10/07/22 and 10/10/22 Non-binding polls extended one day to reach quorum	Ballot Results **(314)** CIP-002-7 **(315)** CIP-003-Y **(316)** CIP-004-8 **(317)** CIP-005-8 **(318)** CIP-006-7 **(319)** CIP-007-7 **(320)** CIP-008-7 **(321)** CIP-009-7 **(322)** CIP-010-5 **(323)** CIP-011-4 **(324)** CIP-013-3 Non-binding Poll Results **(325)** CIP-002-7 **(326)** CIP-003-Y **(327)** CIP-004-8 **(328)** CIP-005-8 **(329)** CIP-006-7 **(330)** CIP-007-7 **(331)** CIP-008-7 **(332)** CIP-009-7 **(333)** CIP-010-5 **(334)** CIP-011-4 **(335)** CIP-013-3	

(302) CIP-004-8 **(303)** CIP-005-8 **(304)** CIP-006-7 **(305)** CIP-007-7 **(306)** CIP-008-7 **(307)** CIP-009-7 **(308)** CIP-010-5 **(309)** CIP-011-4 **(310)** CIP-013-3	Comment Period **(313)** Info (Updated) Submit Comments	08/17/22 - 10/07/22 (Updated 09/09/22)	**(336)** Comments Received	**(337)** Consideration of Comments
Draft 3 CIP-002-7 **(186)** Clean | **(187)** Redline to Last Posted | **(188)** Redline to Last Approved CIP-003-Y **(189)** Clean | **(190)** Redline to Last Posted | **(191)** Redline to Last Approved CIP-004-8 **(192)** Clean | **(193)** Redline to Last Posted | **(194)** Redline to Last Approved CIP-005-8 **(195)** Clean | **(196)** Redline to Last Posted | **(197)** Redline to Last Approved CIP-006-7 **(198)** Clean | **(199)** Redline to Last Posted | **(200)** Redline to Last Approved CIP-007-7 **(201)** Clean - Updated 03/04/22 (SCI added to Part 2.1) Updated 03/09/22 (R4.3 updated with "per system capability") **(202)** Redline to Last Posted - Updated 03/09/22 (R4.3 updated with "per system capability") **(203)** Redline to Last Approved - Updated 03/04/22 (New redlines in the requirement language and SCI added to Part 2.1) Updated 03/09/22 (R4.3 updated with "per system capability") CIP-008-7 **(204)** Clean | **(205)** Redline to Last Posted | **(206)** Redline to Last Approved CIP-009-7 **(207)** Clean | **(208)** Redline to Last Posted | **(209)** Redline to Last Approved CIP-010-5 **(210)** Clean | **(211)** Redline to Last Posted | **(212)** Redline to Last Approved CIP-011-4 **(213)** Clean - Updated 03/09/22 (2.1 updated with "SCI supporting an Applicable System in this Part") **(214)** Redline to Last Posted **(215)** Redline to Last Approved - Updated 03/09/22 (2.1 updated with "SCI supporting an Applicable System in this Part") CIP-013-3 **(216)** Clean | **(217)** Redline to Last Posted | **(218)** Redline to Last Approved Implementation Plan **(219)** Clean | **(220)** Redline **(221)** Proposed New, Modified, and Retired Definitions Used in The Reliability Standards **Supporting Materials** **(222)** Unofficial Comment Form (Word) Technical Rationales **(223)** Definitions and Exemptions **(224)** CIP-002-7 **(225)** CIP-003-Y **(226)** CIP-004-7 **(227)** CIP-005-8 **(228)** CIP-006-7 **(229)** CIP-007-7 **(230)** CIP-008-7 **(231)** CIP-009-7 **(232)** CIP-010-5 **(233)** CIP-011-4 **(234)** CIP-013-3	Additional Ballots and Non-binding Polls **(235)** Updated Info (Ballots Open Reminder) **(236)** Info (Updated)	04/01/22 - 04/12/22 Extended one day to reach quorum	Ballot Results **(239)** CIP-002-7 **(240)** CIP-003-Y **(241)** CIP-004-8 **(242)** CIP-005-8 **(243)** CIP-006-7 **(244)** CIP-007-7 **(245)** CIP-008-7 **(246)** CIP-009-7 **(247)** CIP-010-5 **(248)** CIP-011-4 **(249)** CIP-013-3 Non-binding Poll Results **(250)** CIP-002-7 **(251)** CIP-003-Y **(252)** CIP-004-8 **(253)** CIP-005-8 **(254)** CIP-006-7 **(255)** CIP-007-7 **(256)** CIP-008-7 **(257)** CIP-009-7 **(258)** CIP-010-5 **(259)** CIP-011-4 **(260)** CIP-013-3	
	Comment Period **(237)** Updated Info (Ballots Open Reminder) **(238)** Info (Updated) Submit Comments	02/18/22 - 04/12/22 Extended one day	**(261)** Comments Received	**(262)** Consideration of Comments

Draft 2 CIP-002-7 **(122)** Clean |**(123)** Redline to Last Posted CIP-003-Y **(124)** Clean | **(125)** Redline to Last Posted CIP-004-Y (Updated 07/12/21) **(126)** Clean | **(127)** Redline to Last Posted CIP-005-8 (Updated 07/12/21) **(128)** Clean | **(129)** Redline to Last Posted CIP-006-7 **(130)** Clean | **(131)** Redline to Last Posted CIP-007-7 **(132)** Clean | **(133)** Redline to Last Posted CIP-008-7 **(134)** Clean | **(135)** Redline to Last Posted CIP-009-7 **(136)** Clean | **(137)** Redline to Last Posted CIP-010-5 **(138)** Clean | **(139)** Redline to Last Posted CIP-011-Y **(140)** Clean | **(141)** Redline to Last Posted CIP-013-3 **(142)** Clean | **(143)** Redline to Last Posted **(144)** Implementation Plan **Supporting Materials** **(145)** Unofficial Comment Form (Word) **(146)** Proposed New, Modified, and Retired Definitions Used in The Reliability Standards Technical Rationales **(147)** Definitions and Exemptions **(148)** CIP-002-7 **(149)** CIP-003-Y **(150)** CIP-004-Y **(151)** CIP-005-8 **(152)** CIP-006-7 **(153)** CIP-007-7 **(154)** CIP-008-7 **(155)** CIP-009-7 **(156)** CIP-010-5 **(157)** CIP-011-Y **(158)** CIP-013-3	Additional Ballots and Non-binding Polls **(162)**Updated Info **(163)** Info (Updated 08/05/21) Vote	08/23/21 - 09/01/21 (Updated 08/05/21)	Ballot Results **(164)** CIP-002-7 **(165)** CIP-003-Y **(166)** CIP-004-Y **(167)** CIP-005-8 **(168)** CIP-006-7 **(169)** CIP-007-7 **(170)** CIP-008-7 **(171)** CIP-009-7 **(172)** CIP-010-5 **(173)** CIP-011-Y **(174)** CIP-013-3 Non-binding Poll Results **(175)** CIP-002-7 **(176)** CIP-003-Y **(177)**CIP-004-Y **(178)** CIP-005-8 **(179)** CIP-006-7 **(180)** CIP-007-7 **(181)** CIP-008-7 **(182)** CIP-009-7 **(183)** CIP-010-5 **(184)** CIP-011-Y **(185)** CIP-013-3	
	Comment Period **(159)** Info (Updated 08/05/21) Submit Comments	06/30/21 - 09/01/21 (Updated 08/05/21)	**(160)** Comments Received	**(161)** Consideration of Comments
Draft 1 CIP-002-7 **(58)** Clean | **(59)** Redline CIP-003-9 **(60)** Clean | **(61)** Redline CIP-004-7 **(62)** Clean | **(63)** Redline CIP-005-8 **(64)** Clean | **(65)** Redline CIP-006-7 **(66)** Clean | **(67)** Redline CIP-007-7 **(68)** Clean | **(69)** Redline CIP-008-7 **(70)** Clean | **(71)** Redline CIP-009-7 **(72)** Clean | **(73)** Redline CIP-010-5 **(74)** Clean | **(75)** Redline CIP-011-3 **(76)** Clean | **(77)** Redline	Initial Ballots and Non-binding Polls **(98)** Updated Info **(99)** Info Vote	03/12/21 - 03/22/21	Ballot Results **(100)** CIP-002-7 **(101)** CIP-003-9 **(102)** CIP-004-7 **(103)** CIP-005-8 **(104)** CIP-006-7 **(105)** CIP-007-7 **(106)** CIP-008-7 **(107)** CIP-009-7 **(108)** CIP-010-5 **(109)** CIP-011-3 **(110)** CIP-013-3	

CIP-013-3 **(78)** Clean | **(79)** Redline **(80)** Implementation Plan **Supporting Materials** **(81)** Unofficial Comment Form (Word) **(82)** Proposed New, Modified, and Retired Definitions Used in The Reliability Standards Technical Rationales **(83)** Definitions and Exemptions **(84)** CIP-002-7 **(85)** CIP-003-9 **(86)** CIP-004-7 **(87)** CIP-005-8 **(88)** CIP-006-7 **(89)** CIP-007-7 **(90)** CIP-008-7 **(91)** CIP-009-7 **(92)** CIP-010-5 **(93)** CIP-011-3 **(94)** CIP-013-3			Non-binding Poll Results **(111)** CIP-002-7 **(112)** CIP-003-9 **(113)** CIP-004-7 **(114)** CIP-005-8 **(115)** CIP-006-7 **(116)** CIP-007-7 **(117)** CIP-008-7 **(118)** CIP-009-7 **(119)** CIP-010-5 **(120)** CIP-011-3 **(121)** CIP-013-3	
	Join Ballot Pols (There is a separate ballot and non-binding poll for each of the standards, so it is necessary to join each ballot pool in order to submit votes on all of the standards and their associated Violation Risk Factors and Violation Severity Levels)	01/22/21 - 02/19/21		
	Comment Period **(95)** Info Submit Comments	01/22/21 - 03/22/21	**(96)** Comments Received	**(97)** Consideration of Comments
Final Draft CIP-002-6 Clean | Redline to Last Approved Implementation Plan Clean | Redline to Last Posted	Final Ballot Info Vote	03/26/20 - 04/06/20	Ballot Results	
Draft 4 CIP-002-6 Clean| Redline to Last Posted Implementation Plan **Supporting Materials** Unofficial Comment Form (Word) VRF/VSL Justification	Additional Ballot and Non-binding Poll Updated Info Info Vote	12/06/19 – 12/16/19	Ballot Results Non-binding Poll Results	
	Comment Period Info Submit Comments	11/01/19 – 12/16/19	Comments Received	Consideration of Comments
CIP-005 **(51)** Clean | **(52)** Redline **(53)** Associated Definitions **Supporting Materials** **(54)** Unofficial Comment Form (Word) **(55)** Technical Rationale	Comment Period **(56)** Info Submit Comments	08/09/19 – 09/26/19	**(57)** Comments Received	
Draft 3 CIP-002-6 Clean | Redline to Last Approved (CIP-002-51.a)	Additional Ballot and Non-binding Poll		Ballot Results	

Implementation Plan* **Supporting Materials** Unofficial Comment Form (Word) VRF/VSL Justification* *Due to the amount of redlines that would be reflected from the last approved, these documents are only being posted as clean versions Draft Reliability Standard Audit Worksheet (RSAW) Clean | Redline	Updated Info Info Vote	07/08/19 - 07/17/19	Non-binding Poll Results	
	Comment Period Info Submit Comments	06/03/19 - 07/17/19	Comments Received	Consideration of Comments
	Join Ballot Pools	06/03/19 - 07/02/19		
(45) Virtualization and Future Technologies: Case for Change White Paper **Supporting Materials** **(46)** Unofficial Comment Form (Word) **(47)** Virtualization Case for Change Webinar Q & A	Comment Period **(48)** Info Submit Comments	05/30/19 - 06/28/19	**(49)** Comments Received	**(50)** Consideration of Comments
Final Draft CIP-003-8 Clean | Redline to Last Posted Redline to Last Approved (Updated) Implementation Plan Clean | Redline to Last Posted **Supporting Materials** VRF/VSL Justification Clean | Redline to Last Posted Reliability Standard Audit Worksheet Clean | Redline	Final Ballot Info Vote	04/18/19 - 04/29/19	Ballot Results	
Standard Drafting Team Nominations **Supporting Materials** **(43)** Unofficial Nomination Form (Word)	Nomination Period **(44)** Info Submit Nominations	02/28/19 - 03/29/19		
CIP Virtualization Updates CIP-004-7 **(25)** Clean | **(26)** Redline CIP-005-7 **(27)** Clean | **(28)** Redline CIP-006-7 (Updated documents posted 11/14/18) **(29)** Clean | **(30)** Redline CIP-007-7 **(31)** Clean | **(32)** Redline CIP-010-4 **(33)** Clean | **(34)** Redline **(35)** Definitions (Redline) **Supporting Materials** **(36)** Unofficial Comment Form Technical Rationales **(37)** CIP-005-7 **(38)** CIP-007-7 **(39)** CIP-010-4	Comment Period **(40)** Info Submit Comments	11/02/18 - 12/18/18	**(41)** Comments Received	**(42)** Consideration of Comments
Draft 1	Initial Ballot and Non-binding Poll		Ballot Results	

CIP-002-6 Clean | Redline to Last Posted Implementation Plan Clean | Redline to Last Posted **Supporting Materials** Unofficial Comment Form (Word) VRF/VSL Justification Clean | Redline to Last Posted	Updated Info Info Vote	09/28/18 - 10/09/18	Non-binding Poll Results	
	Comment Period Info Submit Comments	08/23/18 - 10/09/18	Comments Received	
	Join Ballot Pools	08/23/18 - 09/21/18		
Draft 1 CIP-003-8 Clean | Redline to Last Approved Implementation Plan **Supporting Materials** Unofficial Comment Form (Word) VRF/VSL Justification	Initial Ballot and Non-binding Poll Updated Info Info Vote	09/28/18 - 10/09/18	Ballot Results Non-binding Poll Results	
	Comment Period Info Submit Comments	08/23/18 - 10/09/18	Comments Received	Consideration of Comments
	Join Ballot Pools	08/23/18 - 09/21/18		
Final Draft CIP-012-1 Clean | Redline to Last Posted Implementation Plan **Supporting Materials** VRF/VSL Justification Clean | Redline to Last Posted Technical Rationale Clean | Redline to Last Posted Implementation Guidance Clean | Redline to Last Posted Draft Reliability Standard Audit Worksheet (RSAW) Clean | Redline	Final Ballot Info Vote	08/03/18 - 08/13/18	Ballot Results	
Standards Authorization Requests FERC Order No. 843 (Malicious Code Example) IROL Modifications to CIP-002 **Supporting Materials** **Unofficial Comment Forms (Word)** FERC Order No. 843 IROL Modifications to CIP-002	Comment Periods Info Submit Comments	06/14/18 - 07/13/18	Comments Received FERC Order No. 843 (Malicious Code) IROL Modifications to CIP-002	
Draft 4 CIP-012-1 Clean | Redline to Last Posted Implementation Plan **Supporting Materials** Unofficial Comment Form (Word)	Comment Period Info Submit Comments	05/18/18 - 07/03/18	Comments Received	Consideration of Comments
	Additional Ballot and Non-binding Poll	Additional Ballot		

VRF/VSL Justification Clean | Redline to Last Posted Technical Rationale Clean | Redline to Last Posted Implementation Guidance Clean | Redline to Last Posted	Updated Info Info Vote	06/22/18 - 07/03/18 Non-binding Poll 6/22/18 - 7/5/18 Extended to reach quorum	Ballot Results Non-binding Poll Results	
Draft Reliability Standard Audit Worksheet (RSAW) Clean | Redline to Draft 3	Info Send RSAW feedback to: RSAWfeedback@nerc.net			
Standard Drafting Team Nominations **Supporting Materials** **(23)** Unofficial Nomination Form (Word)	Nomination Period **(24)** Info Submit Nominations	04/24/18 - 05/23/18		
Proposed Definition of Control Center Implementation Plan **Supporting Materials** Unofficial Comment Form (Word)	Initial Ballots for the Definition and Implementation Plan Updated Info Info Vote	04/20/18 - 04/30/18	Definition Ballot Results Implementation Plan Ballot Results	
	Comment Period Info Submit Comments	03/16/18 - 04/30/18	Comments Received	Consideration of Comments
	Join Ballot Pools	03/16/18 - 04/16/18		
Draft 2 CIP-002-6 Clean | Redline to Last Approved Implementation Plan Clean | Redline to Last Approved **Supporting Materials** Unofficial Comment Form (Word) VRF/VSL Justification Clean | Redline to Last Posted Consideration of Issues and Directives Clean | Redline to Last Posted	Additional Ballot and Non-binding Poll Updated Info Info Vote	04/20/18 - 04/30/18	Ballot Results Non-binding Poll Results	
	Comment Period Info Submit Comments	03/16/18 - 04/30/18	Comments Received	
Draft Reliability Standard Audit Worksheet (RSAW) Clean | Redline to CIP-002-5.1a	Send RSAW feedback to: RSAWfeedback@nerc.net			
Draft 3 CIP-012-1 Clean | Redline to Last Posted Implementation Plan **Supporting Materials** Unofficial Comment Form (Word)	Additional Ballot and Non-binding Poll Updated Info Info Vote	04/20/18 - 04/30/18	Ballot Results Non-binding Poll Results	

Consideration of Issues and Directives Clean | Redline to Last Posted VRF/VSL Justification Clean | Redline to Last Posted Implementation Guidance Clean | Redline to Last Posted Technical Raionale Clean | Redline to Last Posted Draft Reliability Standard Audit Worksheet (RSAW) Clean | Redline to Draft 2			Comments Received	Consideration of Comments
	Comment Period Info Submit Comments	03/16/18 - 04/30/18		
	Send RSAW feedback to: RSAWfeedback@nerc.net			
Technical Rationale and Justification for CIP-012-1 Implementation Guidance for CIP-012-1 **Supporting Materials** Unofficial Comment Form (Word)	Comment Period Info Submit Comments	11/20/17 - 12/11/17	Comments Received	Consideration of Comments
Draft 2 CIP-012-1 Clean | Redline to Last Posted Implementation Plan Clean | Redline to Last Posted **Supporting Materials** Unofficial Comment Form (Word) Consideration of Issues and Directives Clean | Redline to Last Posted VRF/VSL Justification Clean | Redline to Last Posted Draft Reliability Standard Audit Worksheet (RSAW) Clean | Redline to Last Posted	Additional Ballot and Non-binding Poll Updated Info Info Vote	12/01/17 - 12/11/17 (The Non-binding Poll was extended to 12/12/17 to reach quorum)	Ballot Results Non-Binding Poll Results	Consideration of Comments
	Comment Period Info Submit Comments	10/27/17 - 12/11/17	Comments Received	
	Info Send RSAW feedback to: RSAWfeedback@nerc.net	12/01/17 - 12/11/17		
(20) Virtualization/Unofficial Comment Form (Word)	Comment Period **(21)** Info Submit Comments	10/06/17 - 11/02/17	**(22)** Comments Received	
Draft 1 CIP-002-6 Clean | Redline to Last Approved Implementation Plan **Supporting Materials** Unofficial Comment Form (Word) VRF/VSL Justification Consideration of Issues and Directives Draft Reliability Standard Audit Worksheet (RSAW) Clean | Redline to CIP-002-5.1a	Initial Ballot and Non-binding Poll Updated Info Info Vote	10/20/17 - 10/30/17	Ballot Results Non-binding Poll Results	Consideration of Comments
	Comment Period Info Submit Comments	09/14/17 - 10/30/17	Comments Received	
	Join Ballot Pools	09/14/17 - 10/13/17		
	Info Send RSAW feedback to: RSAWfeedback@nerc.net	10/04/17 - 10/30/17		

Proposed Definition of Control Center Technical Rationale and Justification for CIP-012-1 **Supporting Materials** Unofficial Comment Form - Proposed Definition of Control Center Unofficial Comment Form - Technical Rationale and Justification for CIP-012-1	Comment Periods Info Submit Comments	08/14/17 - 09/12/17	Comments Received Proposed Definition of Control Center Technical Rationale and Justification for CIP-012-1	
Draft 1 CIP-012-1 Implementation Plan **Supporting Materials** Unofficial Comment Form (Word) Consideration of Issues and Directives VRF/VSL Justification	Initial Ballot and Non-binding Poll Updated Info Info Vote	09/01/17 - 09/11/17	Ballot Results Non-binding Poll Results	
	Comment Period Info Submit Comments	07/27/17 - 09/11/17	Comments Received	Consideration of Comments
	Join Ballot Pools	07/27/17 - 08/25/17		
Draft Reliability Standard Audit Worksheet (RSAW)	Info Send RSAW feedback to: RSAWfeedback@nerc.net	08/17/17 - 09/11/17		
TOCC White Paper **Supporting Materials** Unofficial Comment Form (Word)	Comment Period Info Submit Comments	03/14/17 - 04/11/17	Comments Received	
(17) Virtualization/Unofficial Comment Form	Comment Period **(18)** Info Submit Comments	03/14/17 - 04/11/17	**(19)** Comments Received	
Communication Networks/Unofficial Comment Form	Comment Period Info Submit Comments	02/10/17 - 03/13/17	Comments Received	
(14) CIP Exceptional Circumstances/Unofficial Comment Form	Comment Period **(15)** Info Submit Comments	02/10/17 - 03/13/17	**(16)** Comments Received	
Final Draft CIP-003-7(i) Clean | Redline to Last Posted Implementation Plan Clean | Redline to Last Posted Definition of Terms Used in Standards (TCA and Removable Media)	Final Ballots Info Vote	01/30/17 - 02/08/17	Ballot Results CIP-003-7(i) Implementation Plan TCA Definition Removable Media Definition	

Clean | Redline to Last Posted				
Draft 1 CIP-003-7(i) Clean | Redline to Last Approved | Redline to CIP-003-7 Implementation Plan Definition of Terms Used in Standards (TCA and Removable Media) **Supporting Documents** Unofficial Comment Form (Word) VRF/VSL Justification Consideration of Issues and Directives CIP-003-7(i) Draft Reliability Standard Audit Worksheet (RSAW) Updated Clean | Redline to CIP-003-6	Initial Ballots and Non-binding Poll Updated Info Info Vote	01/16/17 - 01/25/17 (The Non-binding Poll was extended to 01/26/17 to reach quorum)	Ballot Results CIP-003-7(i) Implementation Plan TCA Definition Removable Media Definition Non-binding Poll	
	Comment Period Info Submit Comments	12/12/16 - 01/25/17	Comments Received	Consideration of Comments
	Join Ballot Pools The existing CIP-003-7 (LERC) ballot pool was used for all of the ballots associated with this portion of the project. The ballot pools have been re-opened to allow stakeholders to join if they are not existing members.	12/12/16 - 01/10/17		
	Updated Info Send RSAW feedback to: RSAWfeedback@nerc.net	12/27/16 - 01/25/17 Updated RSAW posted January 20, 2017		
Final Draft **CIP-003-7** Clean | Redline to Last Posted Implentation Plan Clean | Redline to Last Posted	Final Ballots Info Vote	12/09/16 - 12/19/16	Ballot Results CIP-003-7 Implementation Plan	
CIP-003-TCA Clean | Redline to CIP-003-6 TCA Implementation Plan **Supporting Documents** Unofficial Comment Form (Word) TCA Consideration of Issues and Directives TCA VRF and VSL Justification TCA Definition	Informal Comment Period Info Submit Comments	11/01/16 - 11/18/16	Comments Received	
Draft 2 **CIP-003-7** Clean | Redline to Last Posted | Redline to Last Approved Implementation Plan Clean | Redline to Last Posted **Supporting Documents**	Additional Ballots and Non-binding Poll Updated Info Info Vote	11/23/16 - 12/05/16	Ballot Results CIP-003-7 Implementation Plan Non-binding Poll	
	Comment Period			

Unofficial Comment Form (Word) VRF and VSL Justification Clean | Redline to Last Posted Consideration of Issues and Directives Clean | Redline to Last Posted	Info Submit Comments	10/21/16 - 12/05/16	Comments Received	Consideration of Comments
CIP-003-7 Draft Reliability Standard Audit Worksheet (RSAW) Clean | Redline	Info Send RSAW feedback to: RSAWfeedback@nerc.net	11/04/16 - 12/05/16		
Draft 1 **CIP-003-7** Clean | Redline to Last Approved **Definition of Term(s) Used in Standards** Clean | Redline	Initial Ballots and Non-binding Poll Updated Info Info Vote	08/26/16 - 09/06/16	Ballot Results CIP-003-7 Implemenation Plan LERC and its Definition Non-binding Poll	
Implementation Plan **Supporting Documents**	Comment Period Info Vote	07/21/16 - 09/06/16	Comments Received	Consideration of Comments
Unofficial Comment Form (Word) VRF and VSL Justification Consideration of Issues and Directives	Join Ballot Pools	07/21/16 - 08/19/16		
Draft CIP-003-7 Reliability Standard Audit Worksheet (RSAW) Clean | Redline	Info Send RSAW Feedback to: RSAWfeedback@nerc.net	08/10/16 - 09/06/16		
The Standards Committee accepted the Standards Authorization Request on July 20, 2016				
Standards Authorization Request **(8)** Clean | **(9)** Redline to Last Posted **Supporting Materials** **(10)** Unofficial Comment Form **(11)** CIP Version 5 Transition Advisory Group Issues for Consideration	Comment Period **(12)** Info Submit Comments	06/01/16 - 06/30/16	**(13)** Comments Received	
(3) Standards Authorization Request **Supporting Materials** **(4)** Unofficial Comment Form (Word) **(5)** CIP Version 5 Transition Advisory Group Issues for Consideration	Comment Period **(6)** Info Submit Comments	03/23/16 - 04/21/16	**(7)**Comments Received	
	Nomination Period			

Supplemental Standard Drafting Team Nominations **Supporting Materials** **(1)** Unofficial Nomination Form (Word)	**(2)** Info	03/10/16 - 03/23/16		

home | account log-in/register | legal and privacy/trademark policy | site map | careers | contact us

Atlanta Office | 3353 Peachtree Road, NE Suite 600 North Tower, Atlanta, GA 30326 | 404-446-2560
Washington Office | 1401 H Street NW, Suite 410, Washington, DC 20005| 202-400-3000

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Supplemental Nomination Period Open through March 23, 2016

Now Available

Nominations are being sought for additional standard drafting team (SDT) members through **8 p.m. Eastern, Wednesday, March 23, 2016**.

Use the electronic form to submit a nomination. If you experience any difficulties in using the electronic form, contact Wendy Muller. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies page and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required.

The time commitment for this project is expected to be significant. Participants should anticipate an average workload of 20 hours per week devoted to the SDT efforts. In person meetings will occur typically for 2 ½ - 3 days most months (not including travel time) and meetings will take place in different parts of North America. When not meeting in person, regularly scheduled conference calls will be used to conduct drafting team work. Outside the scheduled meetings, individuals or subgroups will have additional preparation and support work such as researching and developing proposed concepts, reviewing proposals, compiling comments and drafting responses, etc. Lastly, outreach is an important component of this SDT's effort. Members of the team are expected to interact with other stakeholders during the revision development process.

See the project page and unofficial nomination form for more information.

Next Steps

The Standards Committee is expected to appoint members to the team in April 2016. Nominees will be notified shortly after they have been appointed.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard

Title of Proposed Standard(s):	Modifications to CIP Standards
Date Submitted:	March 9, 2016

SAR Requester Information

Name:	Stephen Crutchfield		
Organization:	NERC		
Telephone:	609-651-9455	E-mail:	Stephen.Crutchfield@nerc.net

SAR Type (Check as many as applicable)

☒ New Standard	☒ Withdrawal of existing Standard
☒ Revision to existing Standard	☐ Urgent Action

SAR Information

Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):

The purpose of this project is to (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the *CIP V5 Issues for Standard Drafting Team Consideration* (V5TAG Transfer Document) and (2) address the Federal Energy Regulatory Commission (Commission) directives contained in Order 822. These revisions will increase reliability and security to the Bulk-Power System (BPS) by enhancing cyber protection of BPS facilities.

Industry Need (What is the industry problem this request is trying to solve?):

The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP version 5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing standard drafting team (SDT) for the CIP Reliability Standards.

SAR Information

The V5 TAG developed the V5TAG Transfer Document to explain the issues and recommend that the SDT consider them in future development activity.

On January 21, 2016, the Commission issued Order No. 822 approving revisions to the CIP version 5 standards and also directing NERC to develop modifications to address:

- Protection of transient electronic devices used at low-impact BES Cyber Systems;
- Protections for communication network components between control centers; and
- Refinement of the Low Impact External Routable Connectivity (LERC) definition.

The Commission did not provide a date by which the modifications for transient devices or communication networks must be completed. For the LERC definition, however, the Commission directed that NERC submit the modification within one year of the effective date of Order No. 822 (March 31, 2017).

Brief Description (Provide a paragraph that describes the scope of this standard action.)

The proposed project will consider the issues raised by the V5TAG in the V5TAG Transfer Document and will address the Commission directives in Order No. 822 through modifications to the CIP standards. The work will include development of Violation Risk Factors, Violation Severity Levels, and an Implementation Plan for the modified standards and will meet the deadlines established by the Commission in Order No. 822.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

As stated above, the purpose of this project is to consider the V5TAG issues in the initial transfer document V5TAG Transfer Document and address the Commission directives contained in Order 822. For the directive on the LERC definition, the project is to respond within the deadline required in the order.

As noted above, the V5TAG identified specific issues with the CIP V5 standards. The V5TAG drafted the V5TAG Transfer Document to formally recommend that the SDT address these issues during standards development to consider whether modifications can be made to the standard language. As outlined in the V5TAG Transfer Document, the specific issues are as follows:

- <u>Cyber Asset and BES Cyber Asset (BCA) Definitions</u> – as foundational definitions within the CIP V5 standards, the understanding of Cyber Asset and BCA terms impacts the scope of the applicable requirements. The V5TAG recommends the following enhancements:
  - Clarify the intent of “programmable” in Cyber Asset.
  - Clarify and focus the definition of “BES Cyber Asset” including:

SAR Information

    - Focusing the definition so that it does not subsume all other cyber asset types.
    - Considering a lower bound to the term 'adverse' in "adverse impact".
    - Clarifying the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that "N-1 contingency" is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.
- Network and Externally Accessible Devices – V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
    - The 4.2.3.2 exemption phrase "between discrete Electronic Security Perimeters"
    - The meaning of the word 'associated' in the ERC definition.
    - The applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section.
    - The IRA definition placement of the phrase "using a routable protocol" in the definition and with respect to Dial-up Connectivity.
    - The Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations – V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:
    - The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
    - The definition of Control Center.
    - The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.
- Virtualization – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider CIP-005 and the definitions of Cyber Asset and Electronic Access Point regarding permitted architecture and the security risks of network, server and storage virtualization technologies.

The SDT shall also address the Order No. 822 directives by developing modifications to requirements in CIP standards and the definition of LERC. The Commission directed the following:

- *Per paragraph 32, "...we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by*

SAR Information
transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards." • *Per paragraph 53, "…the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."* • *Per paragraph 73, "…the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule…."*

Reliability Functions		
The Standard will Apply to the Following Functions (Check each one that applies.)		
☐	Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.

Reliability Functions		
☒	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☒	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and Reactive Power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and Reactive Power supply and demand.

Reliability and Market Interface Principles	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	YES
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	YES
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	YES
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	YES

Related Standards	
Standard No.	Explanation

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
FRCC	
MRO	
NPCC	
RF	
SERC	
SPP RE	
Texas RE	
WECC	

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Standards Authorization Request (SAR)

Do not use this form for submitting comments. Use the electronic form to submit comments on the Project 2016-02 Modifications to CIP Standards SAR. The electronic comment form must be submitted by **8 p.m. Eastern, Thursday, April 21, 2016**.

Documents and information about this project are available on the Project 2016-02 Modifications to CIP Standards. If you have questions, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

Background Information

On January 21, 2016, FERC issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven CIP Reliability Standards and new or modified definitions. FERC also directed NERC to develop modifications to address:

- Protection of transient electronic devices used at low-impact bulk electric system cyber systems;
- Protections for communication network components between control centers; and
- Refinement of the definition for Low Impact External Routable Connectivity (LERC)

FERC directed NERC to submit new or modified standards responding to the directives related to the definition of LERC by March 30, 2016, one year from the effective date of Order No. 822. FERC did not place any time frame for NERC to respond to the remaining directives.

The CIP Version 5 Transition Advisory Group (V5 TAG) transferred issues to the CIP Version 5 Standard Drafting Team (SDT) that were identified during the industry transition to implementation of the CIP Version 5 Standards. Specifically, the issues that the SDT will address are:

- Cyber Asset and BES Cyber Asset Definitions
- Network and Externally Accessible Devices
- Transmission Owner Control Centers Performing Transmission Operator Obligations
- Virtualization

On March 9, 2016, the NERC Standards Committee accepted and authorized the posting of the Modifications to CIP Standards SAR. It is posted for a 30-day informal comment period because it is addressing FERC directives.

Questions

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

   Yes:

   No:

   Comments:

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

   Yes:

   No:

   Comments:

3. Are there any other concerns with this SAR that haven't been covered in previous questions?

   Yes:

   No:

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP V5 Issues for Standard Drafting Team Consideration

September 15, 2015

From experience in the V5 Transition Study and the on-going implementation efforts, the CIP Version 5 Transition Advisory Group (V5TAG) identified specific issues with the CIP Version 5 standard language that caused difficulty in implementation of the requirements. In many cases, the V5TAG members found that select language within the CIP Version 5 standards may be understood in multiple ways. These interpretations appear to go beyond the intended flexibility of the standard language that is necessary to accommodate the diverse nature of facts and circumstances across the electric sector. At this time, the V5TAG proposes the following issues to be addressed by the CIP V5 Revisions drafting team (SDT) or other appropriate team for standards development:

- **<u>Cyber Asset and BES Cyber Asset definitions</u>**
  The foundational definition for the CIP Version 5 standards is 'Cyber Assets.' When Cyber Assets meet a threshold of Bulk Electric System (BES) impact they become 'BES Cyber Assets (BCA)' which are grouped, by a Responsible Entity, into 'BES Cyber Systems (BCS).' Viewing BCAs too broadly can lead to many thousands of devices in the typical utility becoming an administrative burden for which few if any cyber security controls can actually be applied or where there is limited associated cyber security risk. Vast amounts of effort would be expended for these types of cyber assets to track and document their lack of capability for even the most basic cyber security controls. Viewing BCAs too narrowly could lead to missing consideration of devices that have a sufficient level of cyber capability and risk impact.

  The SDT should consider the definition of Cyber Asset and clarify the intent of "programmable" by considering such factors as if a device is merely configurable, its executable code is not field upgradable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc.

  The SDT should consider clarifying and focusing the definition of "BES Cyber Asset" including:
    a. Focusing the definition so that it does not subsume all other cyber asset types. Protected Cyber Assets (PCA), by nature of being on the same network, can have some form of adverse impact if misused. Electronic Access Control or Monitoring Systems (EACMS) if misused or unavailable can have some form of adverse impact. This can result in a "hall of

mirrors” effect where everything in or that creates an Electronic Security Perimeter (ESP) also meets the BCA definition.

   b. Considering if there is a lower bound to the term ‘adverse’ in “adverse impact”. For example, is the focus of a typical generating unit the servers and operator human machine interfaces (HMI) and controller cabinets and Programmable Logic Controllers (PLCs) or is it the thousands of individual sensors and transmitters throughout the plant?
   c. Clarify the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that “N-1 contingency” is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.

- **Network and Externally Accessible Devices (ERC, ESP, IRA)**

  The SDT should consider the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
   a. Clarify the 4.2.3.2 exemption phrase “between discrete Electronic Security Perimeters.” When there is not an ESP at the location, consider clarity that the communication equipment considered out of scope is the same communication equipment that would be considered out of scope if it were between two ESPs.
   b. The word ‘associated’ in the ERC definition is unclear in that it alludes to some form of relationship but does not define the relationship between the items. Striking ‘associated’ and defining the intended relationship would provide much needed clarity.
   c. Review of the applicability of ERC including the concept of the term “directly” used in the phrase “cannot be directly accessed through External Routable Connectivity” within the Applicability section. As well, consider the interplay between IRA and ERC.
   d. Clarify the IRA definition to address the placement of the phrase “using a routable protocol” in the definition and clarity with respect to Dial-up Connectivity.
   e. Address the Guidelines and Technical Basis sentence, “If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.”

- **Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations**

  CIP-002-5.1 Attachment 1 – Impact Reliability Criteria, sections 1.1, 1.2, 1.3, 1.4, 2.11, 2.12, and 2.13 employ the language “used to perform the functional obligation of”, and then lists the functional registration. It was intended that this caveat would capture entities that perform obligations of a specific registered function, whether they are registered for that function or not. However, this language has caused confusion, especially in section 2.12 concerning TOP Control Centers. The term “functional obligation” may be interpreted to have different meaning in a variety of situations.

One interpretation is for the defined term Control Center to be strictly associated with the Balancing Authority (BA), Generator Operator (GOP), Reliability Coordinator (RC), and Transmission Operator (TOP) functional registrations, and that control rooms or dispatch centers owned and operated by Transmission Owners (TOs) with control of limited BES facilities would be excluded. A second interpretation may expand or contract the applicability of the Control Center designation, based on criteria that may not take into consideration overall risk to reliable operations of the BES.

Early analysis found the potential for TOs (not Registered as TOPs) that only operate limited breakers to be pulled in as medium impact Control Centers, even if the few Facilities they control are low impact. (For example, an entity with one 161kV breaker in one substation and a second 161kV breaker in a different substation, both breakers associated with low impact Facilities.) As currently written, low impact Control Centers are to be identified per criteria 3.1 and could be commensurate with risk for these scenarios.

Areas for the SDT to address are:

a. CIP-002-5.1, Attachment 1 Control Center criteria for additional clarity and for possible revisions related to TOP or TO Control Centers performing the functional obligations of a TOP, in particular for small or lower-risk entities. A potential revision could be a size for criteria 2.12, Control Centers performing the functional obligations of a TOP.
b. Clarify the applicability of requirements on a TO Control Center that perform the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES. Review the corresponding Guidelines and Technical Basis of CIP-002-5.1, specifically: the “CIP-002-5” section paragraph starting with “Responsibility for the reliable operation of the BES is spread across all Entity Registrations”; the table following that paragraph; the “High Impact Rating (H)” section; and the criterion bullets for Control Centers under the “Medium Impact Rating (M)” section.
c. The definition of Control Center (if pursued, recognize possible impacts on operations and planning standards and/or glossary terms that include ‘Control Center’, for example, the revised Glossary term for “System Operator” to be effective July 1, 2016).
d. The language scope of “perform the functional obligations of” throughout the Attachment 1 criteria.

- <u>**Virtualization**</u>

  The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration.

> The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies.

The transition to CIP Version 5 continues as the compliance deadline of April 1, 2016 approaches. The V5TAG continues to discuss challenging issues being undertaken during the on-going implementation. The group may find additional issues to transfer to the SDT for consideration.

Standards Announcement

Project 2016-02 Modifications to CIP Standards
Standards Authorization Request

Informal Comment Period Open through April 21, 2016

Now Available

A 30-day informal comment period for the **Project 2016-02** Standard Authorization Request (SAR), is open through **8 p.m. Eastern, Thursday, April 21, 2016**.

Commenting

Use the electronic form to submit comments on the SAR. If you experience any difficulties in using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps

The drafting team will consider all responses received during the comment period and determine the next steps of the project

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

Comments Received Report

Project Name:	2016-02 Modifications to CIP Standards SAR
Comment Period Start Date:	3/23/2016
Comment Period End Date:	4/21/2016
Associated Ballots:	

There were 33 sets of responses, including comments from approximately 33 different people from approximately 32 companies representing 9 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

3. Are there any other concerns with this SAR that haven't been covered in the previous questions?

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Florida Municipal Power Agency	Chris Gowder	3,4,5,6	FRCC	FMPA	Tim Beyrle	Florida Municipal Power Agency	4	FRCC
					Jim Howard	Florida Municipal Power Agency	5	FRCC
					Lynne Mila	Florida Municipal Power Agency	4	FRCC
					Javier Cisneros	Florida Municipal Power Agency	3	FRCC
					Randy Hahn	Florida Municipal Power Agency	3	FRCC
					Don Cuevas	Florida Municipal Power Agency	1	FRCC
					Stan Rzad	Florida Municipal Power Agency	4	FRCC
					Matt Culverhouse	Florida Municipal Power Agency	3	FRCC
					Tom Reedy	Florida Municipal Power Agency	6	FRCC
					Steve Lancaster	Florida Municipal Power Agency	3	FRCC
					Mike Blough	Florida Municipal Power Agency	5	FRCC
					Mark Brown	Florida Municipal Power Agency	4	FRCC

					Chris Adkins	Florida Municipal Power Agency	3	FRCC
					Ginny Beigel	Florida Municipal Power Agency	9	FRCC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Southwest Power Pool, Inc. (RTO)	Jason Smith	2	MRO,SERC,SPP RE,WECC	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Jason Smith	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Ellen Watkins	Southwest Power Pool, Inc. (RTO)	1	SPP RE
					Terri Pyle	Southwest Power Pool, Inc. (RTO)	1,3,5,6	SPP RE
					Mike Buyce	Southwest Power Pool, Inc. (RTO)	1,4	SPP RE
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Robert A. Schaffeld	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Southern Company Services, Inc.	3	SERC
					William D. Shultz	Southern Company - Southern Company Services, Inc.	5	SERC

					John J. Ciza	Southern Company - Southern Company Services, Inc.	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6	NPCC	RSC No Dominion	Paul Malozewski	Northeast Power Coordinating Council	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Brian Shanahan	Northeast Power Coordinating Council	1	NPCC
					Rob Vance	Northeast Power Coordinating Council	1	NPCC
					Mark J. Kenny	Northeast Power Coordinating Council	1	NPCC
					Gregory A. Campoli	Northeast Power Coordinating Council	2	NPCC
					Randy MacDonald	Northeast Power Coordinating Council	2	NPCC
					Wayne Sipperly	Northeast Power Coordinating Council	4	NPCC
					David Ramkalawan	Northeast Power Coordinating Council	4	NPCC

Glen Smith	Northeast Power Coordinating Council	4	NPCC
Brian O'Boyle	Northeast Power Coordinating Council	5	NPCC
Brian Robinson	Northeast Power Coordinating Council	5	NPCC
Bruce Metruck	Northeast Power Coordinating Council	6	NPCC
Alan Adamson	Northeast Power Coordinating Council	7	NPCC
Michael Jones	Northeast Power Coordinating Council	3	NPCC
Michael Forte	Northeast Power Coordinating Council	1	NPCC
Kelly Silver	Northeast Power Coordinating Council	3	NPCC
Brian O'Boyle	Northeast Power Coordinating Council	5	NPCC
Edward Bedder	Northeast Power Coordinating Council	1	NPCC
David Burke	Northeast Power	3	NPCC

						Coordinating Council		
					Peter Yost	Northeast Power Coordinating Council	4	NPCC
					Helen Lainis	Northeast Power Coordinating Council	2	NPCC
					Michele Tondalo	Northeast Power Coordinating Council	1	NPCC
					Kathleen Goodman	Northeast Power Coordinating Council	2	NPCC
					Silvia Parada Mitchell	Northeast Power Coordinating Council	4	NPCC
					Sylvain Clermont	Northeast Power Coordinating Council	1	NPCC
					Si Truc Phan	Northeast Power Coordinating Council	2	NPCC
Colorado Springs Utilities	Shannon Fair	1,3,5,6		Colorado Springs Utilities	Kaleb Brimhall	Colorado Springs Utilities	5	WECC
					Charlie Morgan	Colorado Springs Utilities	3	WECC
					Shawna Speer	Colorado Springs Utilities	1	WECC

					Shannon Fair	Colorado Springs Utilities	6	WECC

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment

The SPP RE respectfully submits the following eight comments to the Project 2016-02 Standards Authorization Request: (1) With respect to clarifying or revising the definition of Cyber Asset, consider including misuse of the Programmable Electronic Device through misconfiguration or reconfiguration of the device in the instance that its behavior is affected and its altered behavior impacts the associated Facility. Consider the risk of misuse (i.e., how would someone misconfigure or reconfigure the device to cause undesired behavior) as appropriate. (2) With respect to clarifying or revising the definition of External Routable Connectivity (ERC), consider the point in the communication path at which a conversion from routable to non-routable communication protocol occurs. Is ERC only established if the conversion occurs in the same asset as the BES Cyber Asset or can ERC be established if the conversion occurs at the remote end of the communication path (e.g., conversion at the Control Center for communication to a serially connected relay in a substation)? Consider whether ERC exists only if the conversion occurs outside of an established ESP (i.e., there is no ERC if the device performing the conversion is inside an ESP and protected per the CIP Standards). (3) With respect to CIP-002-5.1, Impact Rating Criteria 3.2 and 3.3, clarify that the Low Impact BES Cyber Systems are associated with Facilities located within the asset as opposed to being associated with the asset itself. The opening statement in Section 3 of the Impact Rating Criteria states "BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets…" The SPP RE has already been presented with an argument that flow meters in a substation are not BES Cyber Assets because they are associated with a Transmission line and not the Transmission station or substation cited in Impact Rating Criterion 3.2. (4) With respect to Tie Line and other Transmission line flow meters, these Cyber Assets appear to have been unintentionally excluded from consideration under CIP-002-5.1, Impact Rating Criterion 2.5. Impact Rating Criterion 2.5 excludes consideration of BES Cyber Assets associated with Transmission lines through its use of "operating between 200 kV and 499 kV at a single station or substation" language. In the instance where the tie line or other flow meter is associated with a Transmission Line operated between 200 and 499 KV in a substation that satisfies the qualifications of Impact Rating Criterion 2.5, the meter will be excluded and not be categorized as Medium Impacting. Additionally, some entities are proffering the argument that the flow meter is not a BES Cyber Asset because its loss or misuse will not affect the reliable operation of the Transmission Facilities in the substation where the meter resides, overlooking the impact the loss of meter information may have on Control Center operations including ACE calculation, security-constrained generation dispatch, AGC, and Situational Awareness. An additional Criterion, specific to Transmission line flow meters, may be required to address this issue. (5) With respect to Physical Security Perimeters and their associated Requirements, clarification is needed regarding the concept of zoned access within a defined PSP. Specifically, is it acceptable to define an overarching PSP and then establish areas of access control within the defined PSP where BES Cyber Systems are present and for which different access permissions are established? For example, can a building containing a Control Center and its associated data center be declared a single PSP while access controls are established that do not permit all personnel with authorized unescorted access into the building to have authorized unescorted access into one or more access control zones within the building (e.g., the data center). And, if the zoned access areas are deemed to be independent PSPs, would the application of CIP-006-6 R1 Part 1.3 require two access controls to enter the interior PSP containing High Impact BES Cyber Systems, or would the requirement for two access controls to enter the outer (building) PSP suffice such that a single access control is permitted for the interior PSPs? (6) In consideration of the results of the investigation of the Ukraine cyberattack, the SPP RE recommends that Cyber Assets outside of the ESP with a machine-to-machine connection to a Cyber Asset inside the ESP be subjected to the same controls as the Intermediate System. There is a gap in the Standards today whereby a communication protocol typically used for interactive access (e.g., FTP, SSH, web services) can also be used for system-to-system communication. While Interactive Remote Access requires the use of an Intermediate System, encryption, and multi-factor authentication to the

Intermediate System, system-to-system communication using the exact same protocols do not require such controls. The Electronic Access Point cannot tell the difference, thus a successful compromise of the Cyber Asset residing outside of the ESP affords the attacker trusted access into the ESP. (7) In consideration of the results of the investigation of the Ukraine cyberattack, the SPP RE recommends the Standards Drafting Team consider whether essential support systems (UPS, PBX/VOIP phone, fire suppression, emergency generation) should be afforded certain protective controls to mitigate the risk that a successful attack directed at the support systems would adversely impact the asset containing BES Cyber Systems. For example, one element of the Ukraine attack was directed at a network-connected Uninterruptible Power Supply, removing power from essential Cyber Assets. (8) The SPP RE understands that a number of Requests for Interpretation have been submitted against CIP Version 5. While NERC staff has stated publicly that the RFIs would be addressed by the Standards Drafting team, there is no mention of RFIs in the Standards Authorization Request. To the extent that there are RFIs not included in either the Order 822 or V5TAG items, the Standards Authorization Request should state that pending RFIs will be considered and addressed in any revisions to the CIP standards.

Likes 0	
Dislikes 0	

Response

Steven Parker - EnergySec - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

We recommend that the term, Adverse Impact, contained within the BES Cyber Asset definition be itself added as a defined Glossary term. Any attempt to clarify this phrase by adding language within the BES Cyber Asset definition is likely to complicate, rather than simplify, understanding of the term.

The current outstanding Requests For Interpretation should be added as issues to be addressed by the Standards Drafting Team under this SAR. Per the Standards Process Manual, Section 7, Interpretations “shall stand until such time as the Interpretation can be incorporated into a future revision of the Reliability Standard.” Although this statement does not directly apply to the currently open, and unresolved, Requests for Interpretation, we believe the most logical approach would be to address the identified issues via this SAR rather than a separate interpretation development effort.

We recommend that the scope of the SAR be expanded to address the increasing use of 3rd party (i.e. cloud) services. Numerous utilities are leveraging new capabilities available from 3rd party providers in ways that enhance the overall security of the grid. Examples include cloud-based vulnerability scanners, offsite log monitoring services, cloud-based malware analysis and threat detection, cloud-based network monitoring, and colocation facilities. Unfortunately, the current standards are unduly prohibitive towards these services and as a result may be lowering the overall security of the grid by discouraging the use of effective, cutting edge tools, techniques, and services. For example, CIP-006 requires EACMS devices to be within a Physical Security Perimeter. It is not clear how, or if, this requirement can be met for cloud services. The SDT should review existing language and add, modify, or remove language as needed to accommodate any such services that can be prudently deployed to enhance overall grid security.

Likes 0	
Dislikes 0	

Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Xcel Energy has some concern that the SAR’s inclusion of communication network components between control centers could extend to cabling between Control Centers. The inclusion of cabling between Control Centers would be in direct contrast to guidance in the CIP standards and the authority granted in section 215(d)(5) of the FPA by asking entities to be held accountable for equipment they do not own. Communication networks between discrete Electronic Security Perimeters (ESPs) have been excluded from the CIP standards. Additionally, it is unclear how physical protection of cabling would afford any additional protection to networks already in compliance with the suite of CIP standards. Furthermore, the documentation of any physical protection would be administratively burdensome without adding any additional protection. If any requirement is to be added regarding cabling between Control Centers, we would encourage the drafting team to add it as logical controls such as encryption or other such measures under CIP-005 and/or CIP-007. To require physical protection of equipment not owned by Registered Entities seems in direct contrast to previous guidance, outside of the authority documented in section 215(d)(5) of the FPA and add administrate burden with little value.	
Likes 0	
Dislikes 0	
Response	
Ginny Beigel - City of Vero Beach - 9	
Answer	No
Document Name	
Comment	
See response to Question 3.	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
SMUD respectfully suggests an addition to the objective for this SAR be modified to include addressing single points of failure in communication networks and network equipment that meet the definition of the BCA where this equipment is outside of the ESP but contained within the Facility.	
Likes 0	
Dislikes 0	
Response	

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

Seminole concurs with all items currently listed in the draft Standards Authorization Request. Seminole recommends that additional items should be included in the SAR

The industry has received guidance from NERC's Compliance Monitoring and Enforcement group in the form of Frequently Asked Questions and Lessons Learned. These guidance items need to become formal Guidelines, with appropriate Technical Basis, and placed within the Standards and approved by the NERC membership

Issues related to Shared Facilities that are not adequately addressed in the standards. Specifically, when multiple entities have BES Cyber Assets residing at a shared location, there is no clear delineation of responsibility. Without defined responsibilities in the Standard, there is also no documented process to determine who has responsibility and to document those responsibilities. CFRs, JROs, MOUs, and other contractual agreements have been discussed as possible solutions to this issue. However, at a minimum, clear formal Guidelines should be added to CIP-002-5.1. Additional guidance should be added where appropriate.

Based on experience of both the V5TAG and of entities preparing for the standards, it is clear that significant updates are needed to the Guidelines and Technical Basis for all CIP Reliability Standards.

Based on these comments, Seminole recommends adding language to address the following items:

1. **Guidelines and Technical Basis** – As core information used by Entities to ensure a consistent understanding of requirements and based on Lessons Learned by Entities, Reliability Standards CIP-002 through CIP-011 are authorized for modification by the Standards Development Team and submitted for ballot to the NERC Ballot Body. These clarifications should minimally consider
    1. Lessons Learned and FAQs published by NERC and Regional Compliance
    2. Items that may be determined unsupported by the standard and definitions (i.e. BES Reliability Operating Services); and
    3. Industry practices that have evolved from industry's compliance efforts.
2. **Paragraph 51 option** - Option to consider removal of Requirement Parts in specific cases considering the same guidelines as those used in the Paragraph 51 project.
3. **Definitions of Low Impact External Routable Connectivity AND External Routable Connectivity** - Consider modifying the definitions of External Routable Connectivity and LERC to ensure consistent language and communication of both ERC and LERC definitions
4. **Definitions of Cyber Asset, BES Cyber Asset (BCA), and BES Cyber System (BCS)** – The SAR should also authorize changes to clarify the definition of BES Cyber System, specifically whether BES Cyber Systems include any Cyber Asset type other than a BCA (such as PCA, EACMS, PACS)
5. **Measures and Audit Expectations** - Using information provided by the NERC Compliance Monitoring group as one source of information, the measures section of all requirements and requirements parts should be reviewed and updated as necessary to ensure that an entity who provides the evidence listed in the measure is able to fully demonstrate compliance under normal circumstances.
6. **Exceptional Circumstances** - Recommend formalizing guidance for Exceptional Circumstances in a single location.

Likes 0	
Dislikes 0	

Response

Andrew Pusztai - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC is a member of EEI and supports the comments submitted by the EEI CIP Standards Subgroup related to the draft SAR.

Likes 0	

Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The Edison Electric Institute (EEI) submitted comments relating to this SAR. Their comments address scope and objectives of the SAR for consideration by the Standards Drafting Team. Kansas City Power & Light Company endorses and incorporates by reference the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6 - NPCC, Group Name RSC No Dominion	
Answer	No
Document Name	
Comment	
Request that the scope of virtualization be expanded beyond only CIP-005. Want to remind the SDT that communications between Control Centers usually involves third parties that tend to be outside of FERC's jurisdiction.	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	

Comment

The phrase “control centers” in the “Industry Need” section which lists the FERC directives has not been capitalized. FERC Order 822 uses “bulk electric system Control Centers” when speaking about this directive. Tri-State believes the SAR should use that same language used by FERC in order to accurately represent what is expected to be in scope of this project.

There is also an error in the “Reliability Functions” section. “Transmission Service Provider” is checked off instead of “Distribution Provider”. The new versions of the CIP standards do not include Transmission Service Providers, but do include the Distribution Providers.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Virtualization: Manitoba Hydro does not agree with NERC prescribing specific system architecture, technologies or designs. The SDT should continue to focus on identifying requirements to meet specific security objectives for the virtualization.

Protections for communication network components between control centers: Please clarify the scope of Control Centers. Does it refer to the communication links between all Control Centres cross entities such as the link between RC Control Center and TOP Control Centre or only the Control Centers within the resposbile entity.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA is concerned that the Project 2016-02 SAR is too narrowly focused. There are a number of issues with the current CIP Standards, mostly concentrated in CIP-002-5.1. The SAR should be written to allow the drafting team to consider how the suite of CIP standards work together. CIP-002-5.1 is the foundation of the remainder of the CIP requirements. Narrowly scoping this SAR just prolongs dealing with these problems, and ties the drafting team's hands should they identify other concerns. Also, ignoring these issues now will cause more revisions, which in turn will add to the pervasive confusion and uncertainty already surrounding the CIP standards. The industry needs clarity and resolution to these matters in order to be assured their efforts to comply are effective and that companies understand their investments are going to the right places.

The following additional items should be considered by the SDT:

1) Section 4.2.2 states "All BES Facilities" as being subject to the standards for all Responsible Entities except for DP's. This effectively negates the rest of the requirements, as anything that qualifies as a "Cyber Asset" could not possibly be a "Facility" as well. The language is missing the "Cyber Assets" component. Suggested language would be "Cyber Assets at all BES Facilities".

2) Ownership isn't properly accounted for in the requirements. Shared facilities (generally speaking substations) often involve multiple entities that own equipment, who may or may not be Responsible Entities as described in CIP-002-5.1. There should be specific language requiring the owner of the equipment to communicate with the owner of the Facility.

3) Clarify what is meant by "associated with" in the context of the Impact Rating Criteria in CIP-002-5.1 – Attachment 1. Clear up the inconsistencies in the requirements between the use of "associated with" (criterion 2 & 3 in Attachment 1) in some areas and "used by and located at" (criterion 1 in Attachment 1) in other parts. Have a process developed for ensuring entities notify if there are devices owned by a different entity that are "associated with" their BESCS (for example, a meter that one entity needs for the reliable operation of their Control Center that isn't owned by them).

4) Leasing equipment is a loophole in the requirements based on the language in section 4.2. This should be fixed so an entity isn't able to lease equipment and avoid meeting CIP requirements.

5) The scope of equipment applicable to CIP due to applicability to other NERC standards (such as CIP-002-5.1 Section 4.2.1.3) should be clarified further. For example, a "Protection System" can be made up of multiple devices owned by multiple entities. If an entity owns a component of a Protection System that isn't a Cyber Asset, they shouldn't have to meet CIP requirements.

6) Voice over Internet Protocol (VoIP), much like virtualized servers and environments, is not discussed in the CIP requirements. VoIP telephony devices should be excluded from the requirements unless they are networked with other BESCS, in which case they could become protected CA's.

7) There is no mention of "data at rest" in this SAR, although it was clearly part of Order 822 (paragraph 56 – "NERC's response to the directives in this Final Rule should identify the scope of sensitive bulk electric system data that must be protected and specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted **or at rest**").

8) CIP-002-5.1 should be re-written to make sure all assets are properly identified. For example, under R1 of CIP-002-5.1, a Responsible Entity is only required to find Cyber Assets at each of the six locations listed under R1. However, in Attachment 1 for medium and low impact, the language of "associated with" is introduced, indicating that there could be assets/locations containing Cyber Assets that are not part of the list of six asset types listed under R1. The approach taken by R1 is not the one being recommended by NERC or the Regional Entities. The standard should be revised to clarify the relationship between the six asset types/locations in R1 and the "used by and located at"/ "associated with" language in Attachment 1.

Likes 0	
Dislikes 0	

Response

Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	No
Document Name	
Comment	

The SAR should be modified to include the following language and scope:Update obsolete references to NERC defined terms or standards through modifications to the CIP standards. References which are obsolete or require clarification include, but are not limited to:

- To improve consistency within Registered Entity compliance programs, phrasing in CIP-002-5.1 Requirement 1 and Attachment 1 referencing undefined or unclear terms or phrases such as “Transmission stations and substations”, “generation interconnection Facilities”, “Systems and facilities critical to system restoration”, “Generation resources”, “BES reactive resource or group of resources” should be removed by the SDT and instead reference the FERC approved definition of Bulk Electric System (BES) which now included clear and defined qualifications for inclusion and exclusion of these assets as well as an appeals process to address exceptions. An example would be changing the following language:
- R1.ii. Stations and Substations containing BES Facilities
- R1.iii BES Generation Facilities
- RAS: Phrasing in CIP-002-5.1 Applicability, Requirement 1, and Attachment 1 referencing variations of Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements should be clarified and simplified by the SDT to reference the new Remedial Action Scheme (RAS) definition which FERC approved 11/19/2015.
- The current PSP definition should be clarified by the SDT to address that it should not apply to assets in CIP-006-6 Part 1.1 simply because they may be secured in a location which meets the PSP definition: “The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.”
- Interactive Remote Access definition: The SDT should clarify the phrase “system-to-system process communications” to address scripts or batch operations performed on-demand or on a periodic basis as not meeting the definition.
- The phrase “Collector Bus” as it appears in Attachment 1, Criteria 2.4 and 2.5 should be defined by the SDT. The guidance document references a report (*Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface*) which predated the adoption of the NERC BES definition and has not been picked up for development since. The BES definition provides additional clarification of the applicability to multiple generation scenarios in I2, I4, E1, E2, E3, and E4. Notably, CIP-014-1 does provide a diagram of the collector bus, but does not include an associated definition.
- Attachment 1, Criterion 2.4: Clarify if the Transmission Facilities operated at 500kV or higher are “at a single station or substation” to make the language and application consistent with Criterion 2.5 to correctly scope BES Cyber Assets.
- Clarify CIP-002-5.1 R1.vi for Registered Entities registered for additional functions other than Distribution Providers. Revising the language of CIP-002-5.1 R1.vi. to state “*For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above at assets which have not already been considered under Ri-Rv*” would be a possible solution.

Likes 0	
Dislikes 0	
Response	

Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities agrees with the scope of the SAR.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
The Bureau of Reclamation believes that the proposed Standards Authorization Request addresses FERC directives in Order No. 822. Reclamation also supports NERC efforts to address the issues identified by the CIP Version 5 Transition Advisory group.	
Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

Idaho Power agrees with the items that are currently scoped into the SAR, but also believe it does not go far enough. There are numerous areas within the v5/v6 standards where clarifications need to be made. Idaho Power doesn’t think that a full re-write of all of the CIP standards is prudent as it will create continued churn in the industry. Idaho Power believes there should be continual slow improvement in the standards and not large swings that create guidance gaps from the regulators and understanding gaps from the industry.

The proposed scope does not include a change to the applicability columns to tier ratings (i.e., medium with and without ERC). These need to be more explicitly split out as they create odd breakdowns in the standards that seem to be creating inconsistencies in the standards. For example, under CIP-010-2 R4 Attachment 1, R1.2 requires authorizations for all Transient Devices and R3.1 for removable media for Medium Impact BCS. However, Medium Impact BCS without external routable connectivity (ERC) do not require an authorization records under CIP-004, specifically R4.1. This means the critical devices/systems themselves have no authorization requirements, but the transient devices and removable media associated with them do. A second example is information protection for Medium Impact BCS without ERC. CIP-011-2 requires information protection policies/procedures be applied equally to all Medium Impact BCS, which includes protecting it in storage, transit, and use. However, once again, there are no requirements to authorize an individual to gain access to “designated storage locations” under CIP-004-6 Part 4.1.3. This means the information needs to be protected, but only those Medium BCS with ERC have to have individuals get authorized for access to the information. This seems consistent with not authorizing individuals to get access to Medium Impact BCS without ERC but not with applying information protection policies to one tier of Medium Impact BCS.

The SDT should consider four risk tiers rather than three if they are going to treat ERC and non-ERC separately in the standards. These are simply two examples of inconsistencies that have been created by trying to treat them within the same “medium” risk tier. There could still be similar requirements that would be applied to a Medium Impact BCS with ERC and a Medium Impact BCS without ERC, but inconsistencies would be more easily identified by breaking out the Medium BCS tier and the Medium without ERC.

The proposed scope does not include changes to CIP-002-5.1. CIP-002 has several inconsistencies and logic issues and no clearly delineated process allowing no clear way to comply with the standard other than simply deciding on a direction and hoping the regional entity is okay with your approach. The wording and processes required by CIP-002 need to be refined and clarified to make the expectations more clearly known. For example, the Guidelines and Technical Basis state, “The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5.1.” This reference to use of the BROS is stated as an option that may be useful in identifying BCAs/BCSs. Nowhere in CIP-002 the definition of BCA or BCS does it speak directly to the BROS. The only loose tie-in is that the definition of BCS talks about reliability tasks, which FERC, in Order 791, clarified they believed it alluded to the NERC Functional Model, which relates to the high-level responsibilities of registered entities. However, it seems regions are beginning to take a stance that BROS is the hard-line approach as the only acceptable way to approach identification of CIP assets and BCAs/BCSs. Additionally, the wording of the CIP-002 standard does not ever specifically state that an entity needs to identify Protected Cyber Assets (PCAs), Electronic Access Control or Monitoring System (EACMS) or Physical Access Control Systems (PACS), yet the standards expect that entities will know what those devices are in order to apply specific requirements to them. Entities should not have to read between the lines when trying to comply with mandated compliance standards. Doing so creates confusion, inconsistencies, and distrust between the regulators and the industry who should be working together to meet common objectives.

Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT recommends that *Project 2016-02 – Modification to CIP standards* be limited to 1.) clarifying existing language,2.) addressing the V5 TAG issue list, and 3.) incorporating the FERC-directed changes discussed in FERC Order No. 822. Introducing new concepts through substantive language changes in this iteration would be premature. In order to allow CIP Version 5 and 6 concepts to be fully implemented, any proposed substantive changes should be reserved for future CIP standards projects.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Although Austin Energy (AE) agrees with the SAR's objectives, we urge the SDT to proceed with caution. Registered Entities are just now reaching compliance with the Version 5/6 Standards. Unless a device truly creates risk to the BES, we should not include it in the CIP Standards' scope.	
Likes 0	
Dislikes 0	
Response	
Jeri Freimuth - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes

Document Name	

Comment

Arizona Public Service (AZPS) appreciates the opportunity to comment on the proposed SAR. Although AZPS generally supports the scope as described in the SAR, we believe that there are additional clarifications that should be considered beyond those detailed in the FERC Order 822 and the CIP Version 5 Transition Advisory Group (V5TAG) considerations.

AZPS believes the industry would benefit from clarification of the definition of the following terms:

- Transmission Facility – Transmission Facility is not a defined term. Although Facility is a defined term, AZPS does not believe that the Facility definition aligns with the standard’s intent. AZPS suggests that a definition be provided by the Standard Drafting Team (SDT).
- Programmable - The SDT should consider defining programmable to clarify that a device would not be included simply because it was configurable, e.g., has functionality that can be changed locally.

AZPS would also like to suggest that the SDT clarify the intent of the grouping BCAs into BCS by leveraging the logically based perimeter security controls at the Electronic Security Perimeter (ESP) as well as local, device specific security controls per each BES Cyber Asset’s (BCA) capability.

AZPS would also like to add some additional comments to the discussion in the V5TAG CIP V5 Issues for Standard Drafting Team Consideration document.

- AZPS recommends that the SDT consider not defining “adverse impact” or defining a lower bound thereof within the definition of BES Cyber Asset, but to revise the body of CIP standards and/or applicable defined terms to utilize already defined terms such as “Adverse Reliability Impact.” Such would facilitate consistency as well as clarity regarding the N-1 contingency issue and other issues regarding that term identified by the V5TAG.
- AZPS believes that when BES Cyber Assets (BCA), such as relays, RTUs, and others, are connected via serial links to IP converters and/or IP-enabled security gateways, it would be appropriate to consider those elements downstream of the security gateways as BCA that do not have External Routable Connectivity (ERC). This is appropriate because the IP- converters and/or IP-enable security gateways require authentication and provide a protocol break. AZPS believes accurate and timely guidance related to serially connected devices supports the overall goal of providing appropriate and effective cyber security controls; thus, improving reliability.
- AZPS supports the CIP V5TAG analysis regarding virtualization. Virtualization is an effective tool for utilities and consideration should be given to ensuring that flexibility is maintained. An approach should consider the required outcome rather than the specifics of how that outcome is achieved.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF

Answer	Yes
Document Name	
Comment	
Look to NIST 800-125 for virtualization security.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,6,7 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Sistrunk - Small End-Use Electricity Customer - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Smith - Southwest Power Pool, Inc. (RTO) - 2 - MRO,SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

Richard Vine - California ISO - 2

Answer	No
Document Name	

Comment

No comment

Likes 0	
Dislikes 0	

Response

Matt Stryker - Georgia Transmission Corporation - 1 - SERC

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Chris Gowder - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jason Smith - Southwest Power Pool, Inc. (RTO) - 2 - MRO,SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6 - NPCC, Group Name RSC No Dominion	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeri Freimuth - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Chris Sistrunk - Small End-Use Electricity Customer - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,6,7 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginny Beigel - City of Vero Beach - 9	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Parker - EnergySec - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Michael Johnson - Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

3. Are there any other concerns with this SAR that haven’t been covered in the previous questions?	
Warren Cross - ACES Power Marketing - 1,3,5,6 - MRO,WECC,Texas RE,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
The SDT should prioritize the issues based on whether it is associated with a FERC directive or not. For issues that are not directed by FERC, there may need to be additional time to find a resolution associated with these issues. The only deadlines on this project are related to the FERC directives.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erika Doot - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Parker - EnergySec - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	2016-02_CIP_SAR_Unofficial_Comment_Form_ERCOT draft.docx
Comment	
Likes 0	
Dislikes 0	
Response	

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jason Smith - Southwest Power Pool, Inc. (RTO) - 2 - MRO,SPP RE, Group Name SPP Standards Review Group	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Matt Stryker - Georgia Transmission Corporation - 1 - SERC	
Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Michael Johnson - Burns & McDonnell - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

Burns & McDonnell appreciates the opportunity to comment on the Standard Authorization Request (SAR) titled “Modifications to CIP Standards” with the following input:

The V5TAG recommended the Standard Drafting Team (SDT) consider Virtualization as part of the SAR due to the increased use of this technology in industry control system environments. Burns & McDonnell is recommending the Virtualization section of the SAR be amended to indicate that the SDT not only consider virtualization technology usage by Responsibility Entities (Entity) which they own and operate, but usage of similar technology not owned or operated by an Entity. Increased interest in “cloud” based services such as Software as a Service (SaaS) and Platform as a Service (PaaS) have created questions on the application of the standards with no guidance on how they should be applied. Cloud usage of virtual technology is similar to Entity owned usage of the same technology, but Burns & McDonnell feels it is important that both usage conditions be considered and any differences in approach be indicated in any final SDT work product. Burns & McDonnell does not believe a separate section should be created for “cloud” usage, but the SAR section on Virtualization could be updated to cover virtualization technology owned by or usage of services by an Entity. One recommendation for the re-wording is:

The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments either owned and operated by a Responsible Entity, or from a service provider who owns and operates the environment under the service providers control, V5TAG asked that the SDT consider CIP-005 and the definitions of Cyber Asset and Electronic Access Point regarding permitted architecture and the security risks of network, server and storage virtualization technologies under these two type of conditions.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	Yes
Document Name	

Comment	
Currently there are no specific requirements or guidelines included within the NERC CIP Reliability Standards v.5/6 relating to utilization of the cloud. Based on discussions with the regional auditing body, it has been agreed upon that utilization of the cloud for storage of BES Cyber System Information may be sufficiently secured through field level packet encryption with the responsible entity only holding the private key. It would be in the interest of the California ISO for there to be a provision included within the NERC CIP Reliability Standards addressing cloud scenarios.	
Likes 0	
Dislikes 0	
Response	
Ginny Beigel - City of Vero Beach - 9	
Answer	Yes
Document Name	
Comment	

We belong to the FMPA municipal organization and have arrived at a consensus with the help of one of its SMEs who is immersed in CIP Standards. Comments follow below:

The SAR falls short of fixing a lot of the core issues related to CIP-002-5.1. The following additional items should be addressed by the SDT:

1) Section 4.2.2 states “All BES Facilities” as being subject to the standards for all Responsible Entities except for DPs. This effectively negates the rest of the requirements, as anything that qualifies as a “Cyber Asset” could not possibly be a “Facility” as well. The language is missing the “Cyber Assets” component. Suggested language would be “Cyber Assets at all BES Facilities.”

2) Ownership isn’t properly accounted for in the requirements. Shared facilities (generally speaking substations) often involve multiple entities that own equipment, who may or may not be Responsible Entities as described in CIP-002-5.1. There should be specific language requiring the owner of the equipment to communicate with the owner of the Facility.

3) Clarify what is meant by “associated with” in the context of the Impact Rating Criteria in CIP-002-5.1 – Attachment 1. Clear up the inconsistencies in the requirements between the use of “associated with” (criterion 2 & 3 in Attachment 1) in some areas and “used by and located at” (criterion 1 in Attachment 1) in other parts. Have a process developed for ensuring entities notify if there are devices owned by a different entity that are “associated with” their BESCS (for example, a meter that one entity needs for the reliable operation of their Control Center that isn’t owned by them).

4) Leasing equipment is a loophole in the requirements based on the language in section 4.2. This should be fixed so an entity isn't able to lease equipment and avoid meeting CIP requirements.

5) The scope of equipment applicable to CIP due to applicability to other NERC standards (such as CIP-002-5.1 Section 4.2.1.3) should be clarified further. For example, a "Protection System" can be made up of multiple devices owned by multiple entities. If an entity owns a component of a Protection System that isn't a Cyber Asset, they shouldn't have to meet CIP requirements.

6) Voice over Internet Protocol (VoIP), much like virtualized servers and environments, is not discussed in the CIP requirements. VoIP telephony devices should be excluded from the requirements unless they are networked with other BESCS, in which case they could become protected CA's.

7) There is no mention of "data at rest" in this SAR, although it was clearly part of Order 822 (paragraph 56 – "NERC's response to the directives in this Final Rule should identify the scope of sensitive bulk electric system data that must be protected and specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted **or at rest**").

8) CIP-002-5.1 should be re-written to make sure all assets are properly identified. For example, under R1 of CIP-002-5.1, a Responsible Entity is only required to find Cyber Assets at each of the six locations listed under R1. However, in Attachment 1 for medium and low impact, the language of "associated with" is introduced, indicating that there could be assets/locations containing Cyber Assets that are not part of the list of six asset types listed under R1. The approach taken by R1 is not the one being recommended by NERC or the Regional Entities. The standard should be revised to allow for the proper capture of all Cyber Assets either ONLY at the six asset locations, OR both at these locations as well as any other associated location.

Likes 0	
Dislikes 0	
Response	
Diana McMahon - Salt River Project - 1,3,6,7 - WECC	
Answer	Yes
Document Name	
Comment	

For network and externally accessible devices, SRP agrees with improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA). However, SRP has additional concerns.

Although much of CIP-005-5 is compatible to CIP V3 requirements, it does include a new requirement related to IRA for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with ERC. R2.1 states: *Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.*

Based on R2.1 and the defined terms, demonstrating compliance with this requirement fundamentally requires evidence of two items:

1. That an Intermediate System is utilized such that the Cyber Asset initiating IRA does not **“directly access”** an applicable Cyber Asset; and

2. That technology for facilitating IRA meets the definition of an Intermediate System.

Issues with #1 – Ambiguity of “Directly Access”

In SRP’s experience the ERO and Regional Entities have used undefined terminology such as “protocol break”, “OSI layer 7 application break”, “session break” and others to describe what is intended by or compliant with the phrase “does not directly access”. However, SRP believes these terms mean different things to different subject matter experts and auditors. FERC articulated as much in Order 822. Although this issue has focused on LERC/LEAP requirements for low impact assets, the same ambiguity exists in the requirements for high/medium impact facilities. Where standards are unclear or ambiguous, entities are typically afforded flexibility in their compliance approaches. However, SRP believes the ERO has taken a rather prescriptive view of these requirements where reasonable people could easily differ in their interpretation. These ambiguities in defined terms and requirements need to be addressed by the SDT.

Issues with #2 – Ambiguity on acceptable Intermediate Systems

As noted in the Glossary of Terms, an Intermediate System is an Electronic Access Control or Monitoring System (EACMS). That notwithstanding, the ERO and Regional Entities have articulated rather informally and only fairly recently a need to assess each Intermediate System against the definition of BES Cyber Asset. This creates the potential for the proverbial “hall of mirrors” result, in the sense that individuals can rationalize a circumstance where seemingly all Cyber Assets (PACS, EACMS, other) could, under some scenario qualify as a BES Cyber Asset. SRP believes this was clearly not the intent of the Standard Drafting Team, and SRP does not believe this concept was considered for Intermediate Systems evaluated during the CIP V5 pilot project.

Most specifically, an entity that was on the drafting team and participated in the implementation pilot project with no issues was “surprised” with the Regional Entity’s assessment of compliance on this subject at time of audit. There is clearly a disconnect that needs to be addressed.

Architectures to support Interactive Remote Access to high, medium impact control centers, transmission stations and generation resources are very costly. Current ambiguity could cause extensive and rework for high and medium impact systems, and be even more impactful if similar architectures are applied to low impact assets.

The Standards Drafting Team (SDT) must clearly define the term “direct access” for high and medium facilities, ensuring “direct access” has same meaning for low impact facilities as ordered by FERC in its approval of the CIP V5 revisions. To the extent different controls are appropriate for high/medium vs. low impact systems, those distinctions must be clear in the language of the standard. SRP further recommends the SDT re-evaluate the definitions of Interactive Remote Access, Intermediate System, and BES Cyber Asset to ensure entities have a clear understanding of the security and compliance expectations associated with the standards.

Likes 0	
Dislikes 0	

Response

Chris Sistrunk - Small End-Use Electricity Customer - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

I believe that the CIP standards do not properly address security monitoring of networks (routable and non-routable). In my experience in the security industry that breaches (like electric disturbances) are inevitable, even for control systems. It's a matter of when, not if. The Security Event Monitoring logging requirements in CIP 007-5 R4 is a start, but I don't believe this data (4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.) provides enough digital forensic evidence in the aftermath of an intrusion or even a cyber attack. Also, the retention period in 4.3 of a minimum of "90 consecutive calendar days" is not sufficient. According to the 2016 M-Trends Report from FireEye (https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf), the median time of network compromise to discovery of the attacker is 146 days. If a utility only kept 90 days of logs, then it's quite possible that they won't have the forensics data to determine if the attacker used stolen credentials or malicious code. Also, many utilities don't use authentication or encryption with their Control System Protocols such as DNP3, ICCP, and Modbus. If an attacker were to spoof, replay, or modify the SCADA traffic, this would not be detected by the current set of monitoring and logging requirements.

However, IT security best practice of network security montoring (NSM) does provide sufficient network forensics data. NSM is similar to the type of monitoring and visibility required by NERC PRC 002-2 Disturbance Monitoring and Reporting standard. I wrote a blog post (https://www.linkedin.com/pulse/comparing-nerc-disturbance-monitoring-reporting-network-sistrunk) about the similarities between PRC 002-2 and NSM...and how NERC CIP 007 R4 could be improved to provide a bit more forensics data. Collecting NSM type data such as Session Data (timestamp, source IP address, source port, destination IP, destination port at a minimum) does not require a lot of storage space and would provide a better level of visibility. Collecting a shorter time period of full network packet captures for High or Medium BES Cyber Systems (including non-routable dial-up access) also is not very complicated, as IT systems have been doing this a long time.

Since BES systems are becoming more connected, we cannot ignore network security monitoring in the future. I hope it doesn't take a serious cyber incident to convince the need for monitoring...much like the 1965 and 2003 blackouts convinced us to do disturbance monitoring. I know we haven't had a cyber attack that caused a power outage here in North America, but as an Electrical Engineer who has worked in the electric utility industry, now representing the ICS security industry, and also a customer, I want to help ensure that this doesn't happen.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy requests that the SDT consider revisiting the transfer of employees and the requirement to remove access for that employee in 1 calendar day which may be viewed as overly burdensome. While this may be outside the scope of this particular SAR, we feel that since the project is regarding revisions to CIP standards, that we would be remiss not to request further discussion around this topic.	
Likes 0	
Dislikes 0	
Response	
Andrew Pusztai - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
ATC is a member of EEI and supports the comments submitted by the EEI CIP Standards Subgroup realted to the draft SAR. Please review for applicability to this question.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE noticed there is a statement on page 4 which says the compliance deadline is April 1, 2016. This has been moved back to July 1, 2016.	

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

In addition to the issues addressed by the SAR, the Edison Electric Institute, on behalf of our members, recommends that the proposed project also consider the following ten issues:

Issue 1: CIP Exceptional Circumstances

A CIP Exceptional Circumstance is defined as:

“A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.”

We appreciate the understanding and recognition for the need to enable provisions for CIP Exceptional Circumstances. However, during implementation of CIP V5, it has become apparent that the CIP Exceptional Circumstances provision may need to be added to several requirements. Below are a few situation-based examples:

- *Risk of injury or death*: CIP-004-6 R2 and R4 allow for CIP Exceptional Circumstances to waive the need for Training and the Authorization based on need to be waived during such circumstances. We believe that CIP-004-6 R3 also should allow for CIP Exceptional Circumstances because the requirement to obtain a Personal Risk Assessment takes additional time that would hinder the ability of first responders to enter a Physical Security Perimeter in the event of the need for life saving measures. This would be consistent with CIP-004-3 “except in specified circumstances such as an emergency.”
- *Impediment of large scale workforce availability*: CIP-007-6 R2 Security Patch Management requirements may be difficult to meet in the event that a major storm impacts a responsible entity, which requires all employees to report for storm duty for restoration efforts.
- *Natural disaster*: CIP-006-6 R1 Part 1.4 monitoring may not be possible if the physical access point to a PSP is under water or destroyed by a storm. Similarly, Part 1.3 causes compliance issues if for example, a fire renders a PACS controller panel inoperable and the PSP access points have failed secure. Emergency response may have to use a physical key, mechanical lock, or an axe to gain access. Without the IAC language or CIP Exceptional Circumstance provision, PSP access point monitoring is a zero defect issue.

We recommend that the SDT review all of the requirements of CIP V5 to determine whether: a CIP Exceptional Circumstances provision should be added, the definition of CIP Exceptional Circumstances should be edited, and/or additional explanatory language should be added to the Guidelines and Technical Basis for each standard regarding CIP Exceptional Circumstances.

Issue 2: BES Cyber Asset definition – “redundancy”

The application of the redundancy clause in the BES Cyber Asset (BCA) definition is unclear because the use of different and separate technologies and methods reduce reliability risk by providing alternative data sources. For example, VoIP systems, data center phone systems, radios, and other backup communication systems are alternatives, yet could be considered redundant by auditors and therefore it is unclear whether there are limits to the application of the BCA adverse impact to these systems. Without such limitations, the BCA definition may encourage registered entities to reduce their use of backup/alternative systems to reduce their compliance burdens and risk. While redundant assets may typically have identical security risks and vulnerabilities, requiring both/all to be similarly protected, alternative systems or assets are often substantially different and have drastically dissimilar risks and vulnerabilities, which reduces overall risk to the BES.

Issue 3: VoIP as a BES Cyber Asset

CIP-002-5.1 4.2.3.2 exempts “Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters” from CIP-002-5.1; however, the Guidelines and Technical Basis for CIP-002-5.1 calls out operational directives (TOP, RC, BA) as an aspect of Inter-Entity Coordination and Communication function. As a result, some auditors are viewing VoIP as in scope for CIP-002-5.1 despite the exemption and fact that different and separate communication technologies are used for this function. If the exemption does not apply, then the BES Cyber Asset definition should also apply; however, EEI members are hearing that auditors do not agree and believe that VoIP used for operational directives are BES Cyber Assets even if the 15 minute impact does not apply due to the redundancy issue mentioned above.

We recommend that the SDT consider these issues and determine how best to address VoIP in the standard that is aligned with the risk to the bulk electric system.

Issue 4: LERC definition application to assets located external to the low impact asset

The last three asset classes in CIP-002-5.1 R1 are typically implemented across multiple instances of the first three classes (i.e., systems and facilities critical to system restoration, special protection systems, and distribution provider protection systems are typically implemented at control centers, substations, and generating resources).

The Low Impact External Routable Connectivity (LERC) definition appears to be based on single asset locations (“direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset ***outside the asset*** containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection.”) The phrase “outside the asset” can cause confusion in determining whether LERC exists for these classes of assets that are implemented across multiple sites.

For example, when evaluating a cranking path as an asset to determine if it has LERC, what does “outside the asset” mean? This could also allow for routable protocol based communication within the multiple substation cranking path to not be considered LERC and left unprotected if the entire cranking path is considered a single “asset containing low impact BES Cyber Systems.” It appears these last 3 asset classes are actually criteria that should affect the categorization of the single site asset class where they are implemented.

Issue 5: Custom software (scripts)

CIP-010-2 R1, Part 1.1, subpart 1.1.3 requires a baseline configuration for “any custom software installed.” The Guidelines and Technical Basis for this requirement states that “custom software installed may include scripts developed for local entity functions.” It is unclear whether all scripts must be considered custom software or whether only scripts that can have an impact on the bulk electric system within 15 minutes must be considered custom software under this requirement. A risk-based clarification should be added to this requirement to set boundaries as to what is considered custom software. For example, a script that alters the behavior or function of a BES Cyber Asset or System should be included; however, a script that simply gathers log data, and whose only impact to the BES Cyber Asset is the allocation of incidental CPU cycles, need not be included.

Issue 6: Applicability of the requirement part to Cyber Asset vs. Cyber System

Some requirements such as in the CIP-007-6 standard apply to Cyber Assets within a BES Cyber System (e.g., the R2 security patch management requirements), others apply at either the BES Cyber System level or Cyber Asset level (e.g., the R4 Part 4.1 logging requirements), and others don't specific if they apply at the system or asset level (e.g., R3 Part 3.1 method to deter, detect, or prevent malicious code). Although the applicable systems for each of these requirements is generally the same (i.e., high and medium impact BES Cyber Systems and their associated EACMS, PACS, and PCA), the difference in the requirements language applicability to Cyber Assets, BES Cyber System, or both makes what is necessary to comply with the requirements unclear.

For example, the requirements section for CIP-007-6 R3 Part 3.1 does not specify whether this requirement applies at the BES Cyber System level or Cyber Asset level, therefore it is unclear whether a responsible entity can protect a medium impact BES Cyber System through deploying an anti-virus solution at the BES Cyber System level or whether the entity must deploy the solution at each Cyber Asset to comply with the requirement part. Consistency among the requirements language would be helpful in clearing up this confusion.

Issue 7: Control Center definition

The NERC document titled "CIP V5 Issues for Standard Drafting Team Consideration" already raises issues with the Control Center definition related to Transmission Owner Control Centers; however, it does not address issues related to Generator Operators.

By definition, a Control Center is "one or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers … 4) a Generator Operator for generation Facilities at two or more locations."

Dispersed or distributed generation facilities (e.g., wind, solar, hydro) may not have the traditional control building with a horseshoe operator control desk ("facility hosting operating personnel that monitor and control"). Does the facility have to perform all "real-time … reliability tasks" or as few as one? Does a control room at a single wind farm, which controls a hundred turbines spread over many miles, meet the control center definition or does it become a control center only if it controls multiple wind farms? Also, if personnel maintains the Cyber Assets (e.g., patching or troubleshooting) is this considered "monitor and control" even though they are not personnel performing real-time reliability tasks. Does operating personnel mean those charged with the responsibility to monitor and control the BES or simply personnel who may be located at the generation Facility to maintain the equipment? Also, do each of the "generation Facilities at two or more locations" need to meet the Bulk Electric System definition to be within scope of the Control Center definition? CIP-002-5.1 Requirement R1, iii uses Generation resources, which could be interpreted to include all generation sources, even those that do not meet the Bulk Electric System definition.

As dispersed or distributed generation increases, clarity in language of the standard will become more important.

Issue 8: Security patches for operating Cyber Assets brought into scope under CIP V5

CIP-007-6 R2, Part 2.2 is clear concerning the ongoing evaluation of security patches as of July 1, 2016, but is unclear on what is required for the initial execution of the process ("evaluate security patches for applicability that have been released since the last evaluation") when there is no "last evaluation."

The standard does not require all Systems to be updated by July 1, 2016, but does require a baseline configuration, which includes a listing of all applied patches. The Guidelines and Technical Basis for CIP-010-2 states that "security patches applied would include all patches that have been applied on the cyber asset… CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches." This documentation requirement is particularly burdensome for an asset that has been in service for six years or longer as it requires entities to contact and work closely with their vendors to identify and get historical security patches. Also, documenting all historical patches, especially those that happened years ago will have little, if any impact on reliability.

Issue 9: Guidance for Secure Interactive Remote Access

In the Guidelines and Technical Basis for CIP-005-5, under Requirement R2 it states: “see Secure Remote Access Reference Document (see remote access alert).” Also, the Rationale for R2 states “Additional information is provided in Guidance for Secure Interactive Remote Access published by NERC in July 2011.” We believe these references are to the same document, which is properly titled under the Rationale and note that the 2011 NERC document was written in the context of V3 and not V5. Please evaluate the relevance of this guidance document to the most recent version (currently CIP-005-5). Also please clarify that IRA is intended to address access remotely from outside the organization (i.e., not to include accesses internally between protected networks).

Issue 10: Mistakes in Guidelines and Technical Basis

In implementing CIP V5, we’ve noticed a number of mistakes, which should be addressed, including:

- The rationale statements from the -5 standards were lost in several of the -6 versions of the standards. For example, the second sentence of the CIP-007-5 R2 rationale “The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.” was not carried forward to the -6 Guidelines and Technical Basis, even though there were no changes to the requirement between versions. We recommend reviewing the Rationales in the -6 standards and adding any that were deleted to the Guidelines and Technical Basis of the standard.
- For CIP-007-6 Part 2.2 the Guidelines and Technical Basis states: “Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.” However there are no CIP-007-6 R2 Parts have TFE provisions.
- For CIP-004-6 R4, under the Guidelines and Technical Basis, the Rationale for this requirement states: “to ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. “ ‘Authorization’ should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants ***and included in the delegations referenced in CIP-003-6***” CIP V3 required designating approvers; however this requirement was not included in CIP-003-6 and therefore the emphasized text should be removed***.***
- For CIP-004-6 R4, the Rationale also references “quarterly reviews in Part 4.5”; however there is no Part 4.5 in CIP-004-6 R4.

Likes 0	
Dislikes 0	

Response

Jeri Freimuth - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

NERC’s webpage for this SAR “Project 2016-02 Modifications to CIP Standards”, as of 4/11/2016, states the following:

“Also the scope of this work will incorporate existing and future RFIs relating to the CIP-002 through CIP-011 family of standards.”

AZPS does not believe any RFIs are addressed in the current SAR. We recommend updating the SAR to reference existing submitted RFIs as appropriate. Finally, AZPS recommends removal from the SAR of functional registrations that are no longer included in the Compliance Registry, e.g., Interchange Authority, Load-Serving Entity and Purchasing-Selling Entity.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6 - NPCC, Group Name RSC No Dominion	
Answer	Yes
Document Name	
Comment	
Request that the SAR explicitly reference the correct title of the V5 TAG document, which we believe is “CIP V5 Issues for Standard Drafting Team Consideration, “dated on September 15, 2015.	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Distribution Provider is not checked as an affected Reliability Function.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	
Document Name	4-15-16 DRAFT CIP V5 Implementation Issues.pdf
Comment	
Southern supports the comments of EEI. See attached.	
Likes 0	
Dislikes 0	
Response	

Comments received from Ginette Lacasse, Seattle City Light

Here are our Subject Matter Expert's (SME) comments. Non-italicized text is copied from SAR, with SME additions in RED. Additional SME comments are *in italics*.

Questions

1. **Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.**

Yes:
No: X

Comments:

In several sections the language of the SAR summarizes that of the foundation V5TAG document, but in doing so conflates or glosses over important concepts. Seattle City Light would like to see clarification to the SAR in the following two sections: (added text in red to clarify)

A) Cyber Asset and BES Cyber Asset (BCA) Definitions – as foundational definitions within the CIP V5 standards, the understanding of Cyber Asset and BCA terms impacts the scope of the applicable requirements. 'Right-sizing' the definitions of "Cyber Asset" and "BES Cyber Asset" balances between the administrative burden and negligible security benefit of an overly broad interpretation and the cyber security risk of too narrow an interpretation. The V5TAG recommends the following enhancements:

- Clarify the intent of “programmable” in Cyber Asset.
- Clarify and focus the definition of “BES Cyber Asset” including:
- Focusing the definition so that it does not subsume all other cyber asset types.
- Considering a lower bound to the term ‘adverse’ in “adverse impact”.
- Clarifying the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that “N-1 contingency” is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.

B) Network and Externally Accessible Devices – V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
- The 4.2.3.2 exemption phrase “between discrete Electronic Security Perimeters.” When there is not an ESP at the location, consider clarity that the communication equipment considered out of scope is the same communication equipment that would be considered out of scope if it were between two ESPs.

2 Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

Yes:
No: X

Comments:

3 Are there any other concerns with this SAR that haven’t been covered in previous questions?

Yes: X
No:

Comments*:*

Seattle would like to see the SAR address three additional areas:

A) Clarify those standards and parts where the requirement applies solely to the applicable BES Cyber System, those standards and parts where the requirement applies solely to individual BES Cyber Assets, those where the requirement applies to both BCS and BCA or to either at the option of the responsible entity, and those where the requirement applies to both BCS and BCA or to either depending on the circumstances and configuration.

B) Clarify application of CIP-002-5, in particular the R1 identification of BES Cyber Systems and their association with specific types of assets (small “a”). The linkage is inconsistent: for High impact rating it is any “BCS located at and used by” a Control Center whereas for Medium *impact rating it is any "BCS associated with any of the following," the "following" being a mixed-bag collection of capital "F" Facilities, various systems or groups of Elements, specifically defined terms such as Control Center and Special Protection System, and undefined common-language concepts such as "generation" and "BES reactive resource." Please also clarify the intent of "used by" and "associated with." Does "used by" mean "essential to the operation of," "involved in the operation of," or something else? Does "associated with" combine the concepts of "used by and located at," or would it be sufficient to be either "situated at the physical location of" or "used by"? The present language creates considerable confusion.*

C) Clarify the application of Intermediate System, as discussed by Salt River Project in their comments. Seattle supports Salt River's position and analysis.

Seattle also supports the position that Florida Municipal Power Authority as they submitted in their comments.

Comments received from Kara Douglas – NRG

Questions

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

   Yes:
   No: X
   Comments:

   A) Please consider the definition of Cyber Asset and clarify the intent of the term "Programmable" through consideration of whether a device is merely configurable, its executable code is not field upgradable or field Programmable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc. (which relates to upgrading the executable in the Programmable code and the ability to field program the configuration)

   B) In relation to the terms: "adverse impact" and "control center", NRG proposes that when addressing TO and TOP Control Center functional obligations in CIP-002-5.1 Attachment 1, it also consider addressing similar issues facing Generator Owners (GO) and Generator Operators (GOP). There are GOP "control centers" that do not have traditional control capabilities over generator breakers or output but simply verbally direct generator actions. In this case it is the GOs that perform the actual output changes and breaker operation. Clarifying GO/GOP obligations in tandem with proposed TO/TOP clarification for determining impact is a step forward.

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

Yes:
No: X
Comments:

3. Are there any other concerns with this SAR that haven't been covered in previous questions?

   Yes:
   No: X
   Comments:

Comments received from Marc Donaldson, Tacoma Power

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

   Yes:

   No: X

   Comments: Tacoma Power suggests the following scope changes:

   - SDT should clarify CIP-005 R1 Part 1.5 with respect to encrypted communications, either in the G&TB or, directly within the requirement language.
   - SDT could provide clarity on CIP-002 eliminating ambiguous language ("Facility" vs. "facility" & "location") etc.
   - SDT should clarify whether CIP Exceptional Circumstance exception applies to CIP-004 R3 (PRA). Within the Guidelines and Technical Basis, there is this clarifier "except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response." We suggest the SDT include an exception for CIP Exceptional Circumstance specifically within the requirement language.

2. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standards? If yes, please identify the jurisdiction and specific regulatory requirements.

   Yes:

No: X

Comments:

3. Are there any other concerns with this SAR that haven’t been covered in previous questions?

   Yes:

   No: X

   Comments:

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard

Title of Proposed Standard(s):	Modifications to CIP Standards		
Date Submitted:	June 1, 2016		
SAR Requester Information			
Name:	Stephen Crutchfield		
Organization:	NERC		
Telephone:	609-651-9455	E-mail:	Stephen.Crutchfield@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard ☒ Revision to existing Standard		☒ Withdrawal of existing Standard ☐ Urgent Action	

SAR Information

Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):

The purpose of this project is to (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the *CIP V5 Issues for Standard Drafting Team Consideration* (V5TAG Transfer Document) and (2) address the Federal Energy Regulatory Commission (Commission) directives contained in Order 822. These revisions will increase reliability and security to the Bulk-Power System (BPS) by enhancing cyber protection of BPS facilities.

Industry Need (What is the industry problem this request is trying to solve?):

The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing standard drafting team (SDT) for the CIP Reliability Standards.

SAR Information

The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that the SDT consider them in future development activity.

On January 21, 2016, the Commission issued Order No. 822 approving revisions to the CIP version 5 standards and also directing NERC to develop modifications to address:

- Protection of transient electronic devices used at low-impact BES Cyber Systems;
- Protections for communication network components between control centers; and
- Refinement of the Low Impact External Routable Connectivity (LERC) definition.

The Commission did not provide a date by which the modifications for transient devices or communication networks must be completed. For the LERC definition, however, the Commission directed that NERC submit the modification within one year of the effective date of Order No. 822 (March 31, 2017).

Brief Description (Provide a paragraph that describes the scope of this standard action.)

The proposed project will consider the issues raised by the V5TAG in the V5TAG Transfer Document and will address the Commission directives in Order No. 822 through modifications to the CIP standards. The work will include development of Violation Risk Factors, Violation Severity Levels, and an Implementation Plan for the modified standards and will meet the deadlines established by the Commission in Order No. 822.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

As stated above, the purpose of this project is to consider the V5TAG issues in the initial transfer document V5TAG Transfer Document and address the Commission directives contained in Order 822. For the directive on the LERC definition, the project is to respond within the deadline required in the order.

As noted above, the V5TAG identified specific issues with the CIP V5 standards. The V5TAG drafted the V5TAG Transfer Document to formally recommend that the SDT address these issues during standards development to consider whether modifications can be made to the standard language. As outlined in the V5TAG Transfer Document, the specific issues are as follows:

- <u>Cyber Asset and BES Cyber Asset (BCA) Definitions</u> – as foundational definitions within the CIP V5 standards, the understanding of Cyber Asset and BCA terms impacts the scope of the applicable requirements. The V5TAG recommends the following enhancements:
    - Clarify the intent of “programmable” in Cyber Asset.
    - Clarify and focus the definition of “BES Cyber Asset” including:
        - Focusing the definition so that it does not subsume all other cyber asset types.
        - Considering a lower bound to the term ‘adverse’ in “adverse impact”.

SAR Information

        - Clarifying the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that “N-1 contingency” is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.
- <u>Network and Externally Accessible Devices</u> – V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
    - The 4.2.3.2 exemption phrase “between discrete Electronic Security Perimeters”
    - The meaning of the word ‘associated’ in the ERC definition.
    - The applicability of ERC including the concept of the term “directly” used in the phrase “cannot be directly accessed through External Routable Connectivity” within the Applicability section.
    - The IRA definition placement of the phrase “using a routable protocol” in the definition and with respect to Dial-up Connectivity.
    - The Guidelines and Technical Basis sentence, “If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.”
- <u>Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations</u> – V5TAG is aware of multiple interpretations of the language “used to perform the functional obligation of” in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:
    - The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
    - The definition of Control Center.
    - The language scope of “perform the functional obligations of” throughout the Attachment 1 criteria.
- <u>Virtualization</u> – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of virtualization technologies.

The SDT shall also address the Order No. 822 directives by developing modifications to requirements in CIP standards and the definition of LERC. The Commission directed the following:

- *Per paragraph 32, “...we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission’s concerns, the proposed modifications should be designed to effectively address the risks posed by transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards.”*

SAR Information
- *Per paragraph 53, "…the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."* - *Per paragraph 73, "…the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule…."* In addition, the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions. Finally, the SDT will review the Guidelines and Technical Basis sections of the CIP V5 standards and adjust where appropriate as well as correct any grammatical, punctuation, and/or formatting errors, and make other errata changes to the CIP V5 standards, as necessary.

Reliability Functions		
The Standard will Apply to the Following Functions (Check each one that applies.)		
☐	Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.

Reliability Functions	
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐ Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐ Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒ Transmission Owner	Owns and maintains transmission facilities.
☒ Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒ Distribution Provider	Delivers electrical energy to the End-use customer.
☒ Generator Owner	Owns and maintains generation facilities.
☒ Generator Operator	Operates generation unit(s) to provide real and Reactive Power.
☐ Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐ Market Operator	Interface point for reliability functions with commercial functions.
☐ Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and Reactive Power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	YES
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	YES
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	YES
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	YES

Related Standards

Standard No.	Explanation

Related Standards	

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
FRCC	
MRO	
NPCC	
RF	
SERC	
SPP RE	
Texas RE	
WECC	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved reliability standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard

Title of Proposed Standard(s):	Modifications to CIP Standards		
Date Submitted:	~~March 9~~June 1, 2016		
SAR Requester Information			
Name:	Stephen Crutchfield		
Organization:	NERC		
Telephone:	609-651-9455	E-mail:	Stephen.Crutchfield@nerc.net

SAR Type (Check as many as applicable)

☒ New Standard	☒ Withdrawal of existing Standard
☒ Revision to existing Standard	☐ Urgent Action

SAR Information

Purpose (Describe what the standard action will achieve in support of Bulk Electric System reliability.):

The purpose of this project is to (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the *CIP V5 Issues for Standard Drafting Team Consideration* (V5TAG Transfer Document) and (2) address the Federal Energy Regulatory Commission (Commission) directives contained in Order 822. These revisions will increase reliability and security to the Bulk-Power System (BPS) by enhancing cyber protection of BPS facilities.

Industry Need (What is the industry problem this request is trying to solve?):

The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP ~~version 5~~V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing standard drafting team (SDT) for the CIP Reliability Standards.

SAR Information

The V5~~-~~TAG developed the V5TAG Transfer Document to explain the issues and recommend that the SDT consider them in future development activity.

On January 21, 2016, the Commission issued Order No. 822 approving revisions to the CIP version 5 standards and also directing NERC to develop modifications to address:

- Protection of transient electronic devices used at low-impact BES Cyber Systems;
- Protections for communication network components between control centers; and
- Refinement of the Low Impact External Routable Connectivity (LERC) definition.

The Commission did not provide a date by which the modifications for transient devices or communication networks must be completed. For the LERC definition, however, the Commission directed that NERC submit the modification within one year of the effective date of Order No. 822 (March 31, 2017).

Brief Description (Provide a paragraph that describes the scope of this standard action.)

The proposed project will consider the issues raised by the V5TAG in the V5TAG Transfer Document and will address the Commission directives in Order No. 822 through modifications to the CIP standards. The work will include development of Violation Risk Factors, Violation Severity Levels, and an Implementation Plan for the modified standards and will meet the deadlines established by the Commission in Order No. 822.

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)

As stated above, the purpose of this project is to consider the V5TAG issues in the initial transfer document V5TAG Transfer Document and address the Commission directives contained in Order 822. For the directive on the LERC definition, the project is to respond within the deadline required in the order.

As noted above, the V5TAG identified specific issues with the CIP V5 standards. The V5TAG drafted the V5TAG Transfer Document to formally recommend that the SDT address these issues during standards development to consider whether modifications can be made to the standard language. As outlined in the V5TAG Transfer Document, the specific issues are as follows:

- <u>Cyber Asset and BES Cyber Asset (BCA) Definitions</u> – as foundational definitions within the CIP V5 standards, the understanding of Cyber Asset and BCA terms impacts the scope of the applicable requirements. The V5TAG recommends the following enhancements:
  - Clarify the intent of “programmable” in Cyber Asset.
  - Clarify and focus the definition of “BES Cyber Asset” including:

SAR Information

  - ▪ Focusing the definition so that it does not subsume all other cyber asset types.
  - ▪ Considering a lower bound to the term 'adverse' in "adverse impact".
  - ▪ Clarifying the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that "N-1 contingency" is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.

- Network and Externally Accessible Devices – V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
  - The 4.2.3.2 exemption phrase "between discrete Electronic Security Perimeters"
  - The meaning of the word 'associated' in the ERC definition.
  - The applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section.
  - The IRA definition placement of the phrase "using a routable protocol" in the definition and with respect to Dial-up Connectivity.
  - The Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."
- Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations – V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:
  - The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
  - The definition of Control Center.
  - The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.
- Virtualization – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider the CIP~~-005~~ V5 standards and the associated definitions ~~of Cyber Asset and Electronic Access Point~~ regarding permitted architecture and the security risks of ~~network, server and storage~~ virtualization technologies.

The SDT shall also address the Order No. 822 directives by developing modifications to requirements in CIP standards and the definition of LERC. The Commission directed the following:

- *Per paragraph 32, "...we direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability. While NERC has flexibility in the manner in which it addresses the Commission's concerns, the proposed modifications should be designed to effectively address the risks posed by*

SAR Information
transient devices to Low Impact BES Cyber Systems in a manner that is consistent with the risk-based approach reflected in the CIP version 5 Standards." - *Per paragraph 53, "…the Commission concludes that modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. Therefore, we adopt the NOPR proposal and direct that NERC, pursuant to section 215(d)(5) of the FPA, develop modifications to the CIP Reliability Standards to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the bulk electric system by the assets being protected (i.e., high, medium, or low impact)."* - *Per paragraph 73, "…the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term "direct" as it is used in the proposed definition. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop a modification to provide the needed clarity, within one year of the effective date of this Final Rule…."* In addition, the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions. Finally, the SDT will review the Guidelines and Technical Basis sections of the CIP V5 standards and adjust where appropriate as well as correct any grammatical, punctuation, and/or formatting errors, and make other errata changes to the CIP V5 standards, as necessary.

Reliability Functions		
The Standard will Apply to the Following Functions (Check each one that applies.)		
☐	Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.

Reliability Functions	
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☒ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐ Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
~~☒~~ ☐ Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒ Transmission Owner	Owns and maintains transmission facilities.
☒ Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
~~☐~~ ☒ Distribution Provider	Delivers electrical energy to the End-use customer.
☒ Generator Owner	Owns and maintains generation facilities.
☒ Generator Operator	Operates generation unit(s) to provide real and Reactive Power.
☐ Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐ Market Operator	Interface point for reliability functions with commercial functions.
☐ Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and Reactive Power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	YES
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	YES
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	YES
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	YES

Related Standards	
Standard No.	Explanation

Related Standards	

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
FRCC	
MRO	
NPCC	
RF	
SERC	
SPP RE	
Texas RE	
WECC	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards Standards Authorization Request (SAR)

Do not use this form for submitting comments. Use the electronic form to submit comments on the **Project 2016-02 Modifications to CIP Standards SAR**. The electronic comment form must be submitted by **8 p.m. Eastern, Thursday, June 30, 2016**.

Additional information about this project is available on the Project 2016-02 Modifications to CIP Standards page. If you have questions, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

Background Information

On January 21, 2016, the Commission issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven CIP Reliability Standards and new or modified definitions. On March 9, 2016, the NERC Standards Committee accepted the Standards Authorization Request (SAR) and authorized the posting of the Modifications to CIP Standards SAR. It was posted for a 30-day informal comment period March 23 – April 21, 2016. Based on the comments received, the Standard Drafting Team (SDT) made minor revisions to the SAR which will be posted for an additional 30-day informal comment period.

It was noted in the comments received on the SAR that the Virtualization issue involved more than just CIP-005 standards and the defined terms Cyber Asset and Electronic Access Point. To correct this, the SDT revised the sentence to: "Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider ~~CIP-005 and the definitions of Cyber Asset and Electronic Access Point~~ the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of ~~network, server and storage~~ virtualization technologies."

Other commenters suggested that the SDT include provisions to address CIP Exceptional Circumstances. A sentence was added to the SAR to include this topic: "In addition, the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions."

A sentence was also added to the SAR allowing the SDT to make errata changes to the standards as necessary and to correct grammatical, punctuation and/or formatting errors in the V5 Standards: "Finally, the SDT will review the Guidelines and Technical Basis sections of the CIP V5 standards and adjust where appropriate as well as correct any grammatical, punctuation, and/or formatting errors, and make other errata changes to the CIP V5 standards, as necessary."

In the previous version of the SAR, the Transmission Service Provide (TSP) Reliability Function was checked as an applicable function. The TSP is not applicable under the CIP standards and this function was corrected by unchecking the TSP Reliability Function in this version of the SAR. Similarly, the Distribution

Provider (DP) Reliability Function was left unchecked in the original SAR. The CIP Standards apply to the DP, so this was corrected by checking the DP Reliability Function in this version of the SAR.

Questions

1. The CIP SDT revised the SAR based on the comments received in the previous posting as noted above. Do you agree with these revisions to the SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

   Yes:

   No:

   Comments:

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP V5 Issues for Standard Drafting Team Consideration

September 15, 2015

From experience in the V5 Transition Study and the on-going implementation efforts, the CIP Version 5 Transition Advisory Group (V5TAG) identified specific issues with the CIP Version 5 standard language that caused difficulty in implementation of the requirements. In many cases, the V5TAG members found that select language within the CIP Version 5 standards may be understood in multiple ways. These interpretations appear to go beyond the intended flexibility of the standard language that is necessary to accommodate the diverse nature of facts and circumstances across the electric sector. At this time, the V5TAG proposes the following issues to be addressed by the CIP V5 Revisions drafting team (SDT) or other appropriate team for standards development:

- **Cyber Asset and BES Cyber Asset definitions**
  The foundational definition for the CIP Version 5 standards is 'Cyber Assets.' When Cyber Assets meet a threshold of Bulk Electric System (BES) impact they become 'BES Cyber Assets (BCA)' which are grouped, by a Responsible Entity, into 'BES Cyber Systems (BCS).' Viewing BCAs too broadly can lead to many thousands of devices in the typical utility becoming an administrative burden for which few if any cyber security controls can actually be applied or where there is limited associated cyber security risk. Vast amounts of effort would be expended for these types of cyber assets to track and document their lack of capability for even the most basic cyber security controls. Viewing BCAs too narrowly could lead to missing consideration of devices that have a sufficient level of cyber capability and risk impact.

  The SDT should consider the definition of Cyber Asset and clarify the intent of "programmable" by considering such factors as if a device is merely configurable, its executable code is not field upgradable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc.

  The SDT should consider clarifying and focusing the definition of "BES Cyber Asset" including:
    a. Focusing the definition so that it does not subsume all other cyber asset types. Protected Cyber Assets (PCA), by nature of being on the same network, can have some form of adverse impact if misused. Electronic Access Control or Monitoring Systems (EACMS) if misused or unavailable can have some form of adverse impact. This can result in a "hall of

mirrors" effect where everything in or that creates an Electronic Security Perimeter (ESP) also meets the BCA definition.

  b. Considering if there is a lower bound to the term 'adverse' in "adverse impact". For example, is the focus of a typical generating unit the servers and operator human machine interfaces (HMI) and controller cabinets and Programmable Logic Controllers (PLCs) or is it the thousands of individual sensors and transmitters throughout the plant?
  c. Clarify the double impact criteria (cyber asset affects a facility and that facility affects the reliable operation of the BES) such that "N-1 contingency" is not a valid methodology that can eliminate an entire site and all of its Cyber Assets from scope.

- **Network and Externally Accessible Devices (ERC, ESP, IRA)**

  The SDT should consider the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:
  a. Clarify the 4.2.3.2 exemption phrase "between discrete Electronic Security Perimeters." When there is not an ESP at the location, consider clarity that the communication equipment considered out of scope is the same communication equipment that would be considered out of scope if it were between two ESPs.
  b. The word 'associated' in the ERC definition is unclear in that it alludes to some form of relationship but does not define the relationship between the items. Striking 'associated' and defining the intended relationship would provide much needed clarity.
  c. Review of the applicability of ERC including the concept of the term "directly" used in the phrase "cannot be directly accessed through External Routable Connectivity" within the Applicability section. As well, consider the interplay between IRA and ERC.
  d. Clarify the IRA definition to address the placement of the phrase "using a routable protocol" in the definition and clarity with respect to Dial-up Connectivity.
  e. Address the Guidelines and Technical Basis sentence, "If dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies."

- **Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations**

  CIP-002-5.1 Attachment 1 – Impact Reliability Criteria, sections 1.1, 1.2, 1.3, 1.4, 2.11, 2.12, and 2.13 employ the language "used to perform the functional obligation of", and then lists the functional registration. It was intended that this caveat would capture entities that perform obligations of a specific registered function, whether they are registered for that function or not. However, this language has caused confusion, especially in section 2.12 concerning TOP Control Centers. The term "functional obligation" may be interpreted to have different meaning in a variety of situations.

One interpretation is for the defined term Control Center to be strictly associated with the Balancing Authority (BA), Generator Operator (GOP), Reliability Coordinator (RC), and Transmission Operator (TOP) functional registrations, and that control rooms or dispatch centers owned and operated by Transmission Owners (TOs) with control of limited BES facilities would be excluded. A second interpretation may expand or contract the applicability of the Control Center designation, based on criteria that may not take into consideration overall risk to reliable operations of the BES.

Early analysis found the potential for TOs (not Registered as TOPs) that only operate limited breakers to be pulled in as medium impact Control Centers, even if the few Facilities they control are low impact. (For example, an entity with one 161kV breaker in one substation and a second 161kV breaker in a different substation, both breakers associated with low impact Facilities.) As currently written, low impact Control Centers are to be identified per criteria 3.1 and could be commensurate with risk for these scenarios.

Areas for the SDT to address are:

a. CIP-002-5.1, Attachment 1 Control Center criteria for additional clarity and for possible revisions related to TOP or TO Control Centers performing the functional obligations of a TOP, in particular for small or lower-risk entities. A potential revision could be a size for criteria 2.12, Control Centers performing the functional obligations of a TOP.
b. Clarify the applicability of requirements on a TO Control Center that perform the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES. Review the corresponding Guidelines and Technical Basis of CIP-002-5.1, specifically: the “CIP-002-5” section paragraph starting with “Responsibility for the reliable operation of the BES is spread across all Entity Registrations”; the table following that paragraph; the “High Impact Rating (H)” section; and the criterion bullets for Control Centers under the “Medium Impact Rating (M)” section.
c. The definition of Control Center (if pursued, recognize possible impacts on operations and planning standards and/or glossary terms that include ‘Control Center’, for example, the revised Glossary term for “System Operator” to be effective July 1, 2016).
d. The language scope of “perform the functional obligations of” throughout the Attachment 1 criteria.

- **Virtualization**

  The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration.

> The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies.

The transition to CIP Version 5 continues as the compliance deadline of April 1, 2016 approaches. The V5TAG continues to discuss challenging issues being undertaken during the on-going implementation. The group may find additional issues to transfer to the SDT for consideration.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards
Standards Authorization Request

Informal Comment Period Open through June 30, 2016

Now Available

A 30-day informal comment period for the **Project 2016-02 Standards Authorization Request (SAR)**, is open through **8 p.m. Eastern, Thursday, June 30, 2016**.

Commenting
Use the electronic form to submit comments on the SAR. If you experience any difficulties in using the electronic form, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps
The drafting team will review all responses received during the comment period and determine the next steps of the project

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact either Senior Standards Developer, Stephen Crutchfield at (609) 651-9455 or Al McMeekin at (404) 446-9675.

Comment Report

Project Name: 2016-02 Modifications to CIP Standards SAR June 2016

Comment Period Start Date: 6/1/2016

Comment Period End Date: 6/30/2016

Associated Ballots:

There were 21 sets of responses, including comments from approximately 21 different people from approximately 21 companies representing 8 of the Industry Segments as shown in the table on the following pages.

Questions

1. The CIP SDT revised the SAR based on the comments received in the previous posting as noted above. Do you agree with these revisions to the SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
MRO	Emily Rousseau	1,2,3,4,5,6	MRO	MRO-NERC Standards Review Forum (NSRF)	Joe Depoorter	Madison Gas & Electric	3,4,5,6	MRO
					Chuck Lawrence	American Transmission Company	1	MRO
					Chuck Wicklund	Otter Tail Power Company	1,3,5	MRO
					Dave Rudolph	Basin Electric Power Cooperative	1,3,5,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Jodi Jenson	Western Area Power Administration	1,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Mahmood Safi	Omaha Public Utility District	1,3,5,6	MRO
					Shannon Weaver	Midwest ISO Inc.	2	MRO
					Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Brad Perrett	Minnesota Power	1,5	MRO
					Scott Nickels	Rochester Public Utilities	4	MRO
					Terry Harbour	MidAmerican Energy Company	1,3,5,6	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,4,5,6	MRO

					Tony Eddleman	Nebraska Public Power District	1,3,5	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
BC Hydro and Power Authority	Patricia Robertson	1,2,3,5		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC
					Venkataramakrishnan Vinnakota	BC Hydro and Power Authority	2	WECC
					Pat G. Harrington	BC Hydro and Power Authority	3	WECC
					Clement Ma	BC Hydro and Power Authority	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7	NPCC	RSC	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Mark J. Kenny	Eversource Energy	1	NPCC
					Gregory A. Campoli	NY-ISO	2	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC

					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Brian Shanahan	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					Michael Forte	Con-Edison	1	NPCC
					Kelly Silver	Con-Edison	3	NPCC
					Peter Yost	Con-Edison	4	NPCC
					Sean Bodkin	Dominion	4	NPCC
					Silvia Parada Mitchell	NextEra Energy	4	NPCC
					Brian O'Boyle	Con-Edison	5	NPCC
					Kathleen M. Goodman	ISO-NE	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
Colorado Springs Utilities	Shannon Fair	1,3,5,6		Colorado Springs Utilities	Kaleb Brimhall	Colorado Springs Utilities	5	WECC
					Charlie Morgan	Colorado Springs Utilities	3	WECC
					Shawna Speer	Colorado Springs Utilities	1	WECC
					Shannon Fair	Colorado Springs Utilities	6	WECC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Jason Smith	Southwest Power Pool Inc	2	SPP RE

					Kim VanBrimer	Southwest Power Pool Inc	2	SPP RE
					John Allen	City Utilities of Springfield	1,4	SPP RE
					Mike Buyce	City Utilities of Springfield	1,4	SPP RE
					Paul Mehlhaff	Sunflower Electric Power Corporation	1	SPP RE
					TARA Lightner	Sunflower Electric Power Corporation	1	SPP RE
ACES Power Marketing	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Brazos Electric Power Cooperative, Inc.	BREC	1,5	Texas RE
					Western Farmers Electric Cooperative	WFEC	1,5	SPP RE
					Old Dominion Electric Cooperative	ODEC	3,4	SERC
					Golden Spread Electric Cooperative	GSEC	5	SPP RE
					Prairie Power, Inc.	PPI	1,3	SERC
					Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF

1. The CIP SDT revised the SAR based on the comments received in the previous posting as noted above. Do you agree with these revisions to the SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.	
Bob Reynolds - 10	
Answer	No
Document Name	
Comment	
The SPP RE respectfully submits the following two comments to the Project 2016-02 Standards Authorization Request: (1) Reference the comments submitted by the SPP Regional Entity (SPP RE) April 2016. In those comments, the SPP RE pointed out that Tie Line and other Transmission line flow meters appear to have been unintentionally excluded from consideration under CIP-002-5.1, Impact Rating Criterion 2.5. This significant issue does not appear to have been included in the revised SAR. The original SPP RE comment is restated here: “Impact Rating Criterion 2.5 excludes consideration of BES Cyber Assets associated with Transmission lines through its use of “operating between 200 kV and 499 kV at a single station or substation” language. In the instance where the tie line or other flow meter is associated with a Transmission Line operated between 200 and 499 KV in a substation that satisfies the qualifications of Impact Rating Criterion 2.5, the meter will be excluded and not be categorized as Medium Impacting. Additionally, some entities are proffering the argument that the flow meter is not a BES Cyber Asset because its loss or misuse will not affect the reliable operation of the Transmission Facilities in the substation where the meter resides, overlooking the impact the loss of meter information may have on Control Center operations including ACE calculation, security-constrained generation dispatch, AGC, and Situational Awareness. An additional Criterion, specific to Transmission line flow meters, may be required to address this issue.” (2) The SPP RE notes that the revised SAR still makes no mention of the consideration of submitted and outstanding Requests for Interpretation. NERC staff has stated publicly that the RFIs would be addressed by the Standards Drafting Team. The SPP RE is aware that at least one of the issues discussed in the April 2016 comments to the SAR has been formally submitted as a Request for Interpretation. To fail to consider outstanding RFIs in the course of modifying the CIP Standards under this SAR would be a missed opportunity to address significant confusion regarding the expectations of the Requirements under question.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - 1,3,5,6	
Answer	No
Document Name	
Comment	
For virtualization, Manitoba Hydro does not agree with NERC prescribing specific system architecture, technologies or designs. SDT should continue to focus on identifying requirements to meet specific objectives for the virtualization. Manitoba Hydro agrees with adding more CIP V5 requirements exceptions for CIP Exceptional Circumstance.	
Likes 0	
Dislikes 0	

Response

Emily Rousseau - 1,2,3,4,5,6 - MRO, Group Name MRO-NERC Standards Review Forum (NSRF)

Answer	No
Document Name	

Comment

The NSRF agrees with the drafting team’s addition of “reviewing and addressing the CIP V5 requirements for CIP Exceptional Circumstances exceptions” to the SAR. However, we request clarification on the scope of Guidelines and Technical Basis sections that may be changed with updates to the associated Standards within this project. We believe that addressing all CIP V5 Guidelines and Technical Basis sections within the scope of this revision may make the project unwieldy as it already contains a substantial scope of work to address FERC directives. We suggest that only Guidelines and Technical Basis sections related to standards language updates should be addressed within the scope of this project.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - 1,2,3,5, Group Name BC Hydro

Answer	No
Document Name	

Comment

CIP-002-5.1

A) The topic of adverse impact should provide more clarity on the real-time requirement as well.

B) Per Medium Impact criterion 2.3 for generation resources, need further clarity on the extent of planning horizon > 1 year contingencies to consider regarding the determination of BES Adverse Reliability Impacts to a given Interconnection. The Guidelines and Technical basis of CIP-002-5.1 reference as an example, TPL-003 Category C3 contingency system studies but otherwise, there is no lower or upper limit indicated regarding the depth of contingencies to be considered. The limit is currently subjective for Transmission Planners and Planning Coordinators.

Furthermore, per the definition of Adverse Reliability Impact, there is direct reference to impacts on a given Interconnection but it is not clear whether this is only considering inter-tie paths or general BES impacts beyond a specific BES location (i.e. generation plant or substation). The Guidelines and Technical basis state only widespread impacts are to be considered instead of localized impacts but it is not clear what is considered ‘widespread’.

CIP-005-5 The fundamental concepts of the intermediate system are omitted or subjective. The standards should define what the requirements are for this system, whether it is strictly a jump host (not mentioned in the standards) or can have more functionality (i.e. software installed upon it). This should be included in the ’Network and Externally Accessible Devices’ section.

CIP-005-5/CIP-003-6 A clear exemption is given for low impact systems is given in CIP-003-6 Guidelines and Technical Basis (CIP-006-6 pg 28) “To future-proof the standards, and in order to avoid future technology issues, the definitions specifically exclude “point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems,” such as IEC 61850 messaging.” The ‘Network and Externally Accessible Device’” section should address this topic for medium impact BCS/BCA as well. These technologies are not limited to low impact systems and guidance should be provided.

CIP-007-5: Regarding security patch applications and cyber vulnerability assessments:

- Certain legacy devices (i.e. HMIs, PLCs, etc.) can be in a “fragile” state and are at high-risk regarding the application of software updates, which include cyber security related updates. There is a demonstrable risk in breaking their functionality which can have an adverse impact on the BES as the only solution is to replace the device entirely or at best, perform a complete reset of the device. This is mainly due to bugs that could be introduced by vendors through their patches (not enough regression testing done by the vendors) and for which even testing prior to implementation in a production environment may not identify all such bugs prior to implementation. Recommend providing guidance around how to handle the application of cyber security patches to these “fragile” devices and to potentially not mandate security patch applications in all cases where there may be demonstrable evidence of adverse BES impact.

- Further guidance is required within the Guidelines and Technical basis on the exact difference between a ‘paper’ exercise cyber vulnerability assessments (CVA) and ‘active’ CVA with respect to Medium Impact facilities and the extent an entity is expected to go to achieve this. It has been communicated by Regional Entities’ audit approach that paper scans must incorporate some active component to pull configuration settings, etc. from a device for analysis. For legacy devices (namely firmware devices), these active component scans can also pose a risk in breaking the functionality of said devices, which can cause adverse impact to the BES. Recommend including guidance around how to handle CVAs pertaining to these firmware devices without potentially breaking their functionality.

Likes 0	
Dislikes 0	

Response

Chris Mattson - 1,3,4,5,6

Answer	No
Document Name	

Comment

Tacoma asks that the SDT consider removing the final two sentences from the last paragraph of CIP-005-5, Guidelines and Technical Basis, Section 4 – Scope and Applicability of the CIP Cyber Security Standards, Requirement R1. These are shown in bold below for identification:

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. ***Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.***

Tacoma is asking the SDT to consider that there are other methods and technologies for detecting malicious traffic in addition to deep packet inspection. This change to the G&TB would make the standard more consistent with the language in FERC Order No. 706, Paragraph 501 which indicates that it is not the commission’s intent to mandate any specific mechanism to be the second security measure. The language from the FERC order is shown below for reference and the pertinent language is shown in bold:

Paragraph 501. In response to SDG&E and Entergy, in stating that the placement of security measures in front of systems provides a layer of protection for those systems, the Commission was not giving priority to “in front” measures. In fact, the Commission acknowledged in the CIP NOPR that defense *in depth measures are generally integrated within and constitute part of a system or program. In commenting that defense in depth measures may also be effectively placed in front of a system, the Commission intended only to acknowledge that there are multiple ways to implement a defense in depth strategy.* ***The Commission is not mandating any specific mechanism to be the second security measure. We are also not requiring uniformity of security measures, only that each responsible entity have at least two security measures unless it is not technically feasible to do so.*** *The revised CIP Reliability Standard should allow enough flexibility for a responsible entity to take into account each site's specific environment. The Commission believes that this, in conjunction with the allowance of technical feasibility exceptions, alleviates FPL Group's concern that the Commission's proposal is a "one size fits all" approach.*

Also, the SDT should clarify CIP-005 R1 Part 1.5 with respect to encrypted communications either in the G&TB or directly within the requirement language. It important that the SDT clarify how to detect malicious communications when the communications includes encrypted information that is not readily decrypted to allow inspection.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

.

Although Seminole concurs with all items currently listed in the draft Standards Authorization Request, Seminole recommends that additional items should be included in the SAR. Seminole thanks the SAR team for addressing our previous comments, in addition to those of others, related to Exceptional Circumstances and the Guidelines and Technical Basis.

While the changes addressed are necessary to address mandatory requirements from FERC, this SAR does not address the fundamental deficiencies in the current CIP standards. Until these fundamental issues are addressed, the electric sector will continue to struggle implementing the current standard, be faced with inefficiencies in the standard that do not improve cyber and physical security, and have difficulty using new and improved capabilities in a rapidly evolving marketplace.

Seminole recommends adding the following items to the SAR:

1. Update CIP-002 Requirements and the Guidelines and Technical Basis section to clarify the expectations in complying with this standard. Update evidence requirements to make clear the expectations of the standard. Clarify attachment 1 to address V5TAG Lessons Learned and FAQs. Resolve issues in the Guidelines and Technical Basis that are inconsistent with the definition of BES Cyber Asset and BES Cyber System.

2. The SDT will review applicable Standards and Requirements to clarify the SDT's intent for management of shared Facilities when more than one Registered Entity owns Facilities inside a single asset. Interconnections within the BES and with Distribution Providers within a single asset create significant complexity for entities in some regions. This results in a need for a significant number of MOU, CFR, or JRO that both complicates compliance and the audit process.

3. The SDT will review the Measures in the CIP V5 standards and adjust where appropriate to allow an entity that provides evidence consistent with the identified measures to determine compliance if no deficiencies are identified in the provided evidence. This may include modifying measures to match the CIP Version 5 Evidence Request or by clarifying either the measures or Guidelines and Technical basis to clarify intent for adjustment of the evidence request.

Likes 0	
Dislikes 0	

Response

Julie Hall - 6

Answer	No
Document Name	

Comment

Comments: Entergy requests that more detail be provided regarding the actions that will be considered regarding CIP Exceptional Circumstances. Is more specificity regarding what constitutes a CIP Exceptional Circumstance being considered? Is more specificity regarding how to declare and document a CIP Exceptional Circumstance being considered? Will more clarity regarding standards affected by CIP Exceptional Circumstance, including a possible increase of applicable standards, be considered? Some particular questions Entergy has regarding the scope of standards affected by CIP Exceptional Circumstances include:

- CIP-004-5.1 R3 does not include the “except during CIP Exceptional Circumstances” language, yet the Guidelines and Technical Basis section states “Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response.” The language in the Guidelines and Technical Basis seems logical as it may not be feasible to validate PRA’s during a widespread emergency response (i.e. a hurricane) especially when response support is provided by many other companies and/or vendors across the country. It is requested that the “except during CIP Exceptional Circumstances” language be added to the appropriate parts of CIP-004-5.1 R3, particularly CIP-004-5.1 R3 Part 3.5.

- The “except during CIP Exceptional Circumstances” language exists in CIP-006-5 R2 Part 2.1 and Part 2.2 which states that logging and continuous escorting of visitors is not required during CIP Exceptional Circumstances. However, none of the CIP-006-5 R1 parts include the “except during CIP Exceptional Circumstances” language, which in turn requires alerting, monitoring, logging of access approved individuals. This may not be feasible during a widespread event that results in total loss of power at many sites over a widespread geographical area. It is requested that the “except during CIP Exceptional Circumstances” language be added to the appropriate parts of CIP-006-5, particularly R1 to ensure consistency across CIP-006-5.

Likes 0	
Dislikes 0	

Response

Scott Brame - 3,4,5 - SERC

Answer	No
Document Name	

Comment

The following comments are from my CIP SME.

• Per paragraph 73, “…the Commission concludes that a modification to the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6 is necessary to provide needed clarity to the definition and eliminate ambiguity surrounding the term “direct” as it is used in the proposed definition. Therefore, pursuant to section 215(d) (5) of the FPA, we direct NERC to develop a modification.

This is where I believe FERC’s order falls short. Although, the definition for LERC needs to be improved and needs to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6. In my opinion, the requirements for low impact critical assets is incomplete. It appears like the SDT was rushed to provide requirements for low impact. Although, the SDT included some basic requirements for low impact critical assets they should have also included requirements for malware and virus protections. In addition, there should be requirements for logging and auditing of systems and system access. These requirements do not need to be as stringent and comprehensive as what is required for medium and high impact critical assets, but they should also be required for low impact critical assets.

Likes 0	
Dislikes 0	

Response

Warren Cross - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

Thank you for the opportunity to provide comments regarding the Standards Authorization Request (SAR) in response to FERC Directives and v5TAG recommendations. While the current SAR attempts to resolve issues around LERC, virtualization and communication protections, ACES believes the SAR doesn’t adequately detail the areas of concern for LERC and fails to allow for technology advances, which may ultimately hinder industry adoption of more secure solutions to address cyber security threats.

How LERC will be defined based upon the ability to communicate and interactive communication capabilities between Low Impact Facilities that have BES Cyber Assets associated with them has yet to be fully vetted. The ability to communicate with a BES Cyber Asset isn’t the same as interacting with the BES Cyber Asset. This distinction needs to be clearly defined. Another issue for Low Impact BES Cyber Systems is the need for a common definition of when serial devices are in scope and not in scope for consistent industry implementation.

Host-based security applications, advanced security threat analysis services, and cloud-based networks are not in scope for the SAR. There are mechanisms in place in the CIP standards that allow for exceptions, such as TFEs and CIP Exceptional Circumstances. ACES believes that these definitions could be expanded to include technology that exists outside of the standard to be able to be used, with approval, in order to provide the entity with a stronger defense in depth security profile.

If the drafting team proposes to modify definitions, they should consider a process that is non-prescriptive and provides flexibility for registered entities to decide how to best defend against cyber security threats based on their risk analysis. There may be significant advantages for industry to adopt new emerging security applications and cloud based security services. The CIP standards should not limit the tools or technology available to mitigate cyber security risks. We ask the drafting team to consider how the revisions to the CIP standards would allow for the power industry to match the security best practices of other industries against the latest security threats and vulnerabilities. Thank you for your time and attention regarding this SAR.	
Likes 0	
Dislikes 0	
Response	
Erika Doot - 1,5	
Answer	No
Document Name	
Comment	
The Bureau of Reclamation agrees with the drafting team's addition of "reviewing and addressing the CIP V5 requirements for CIP Exceptional Circumstances exceptions" to the SAR. However, Reclamation requests clarification on the scope of Guidelines and Technical Basis sections that may be changed with updates to the associated Standards within this project. Reclamation believes that addressing all CIP V5 Guidelines and Technical Basis sections within the scope of this revision may make the project unwieldy as it already contains a substantial scope of work to address FERC directives. Reclamation suggests that only Guidelines and Technical Basis sections related to standards language updates should be addressed within the scope of this project.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - 1,3,5,6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	

Comment	
CSU supports the standard dradting teams updates to the SAR.	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - 3,5	
Answer	Yes
Document Name	
Comment	
AEP suggests that the SDT include separate balloting and commenting for Guidelines and Technical Basis throughout this project. With the development of implementation guidance, AEP is unsure whether the Guidelines and Technical Basis document should remain a part of the codified Reliability Standard. If it does, then stakeholders should have the ability to vote and comment on the contents specifically.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
As our review group evaluated the revised SAR, we noticed that the V5TAG recommends providing clarity in the definitions of the two terms ‘External Routable Connectivity (ERC)’ and ‘Interactive Remote Access (IRA). We suggest the drafting team either develop a new SAR or modify this one in order to require the term ‘External Routable Connectivity (ERC)’ to have the acronym and revised definition updated in the NERC Glossary and also included in the Rules of Procedure (RoP) for consistency and proper alignment. Additionally, we suggest the drafting team edit the SAR to review the Rules of Procedure where the acronym (IRA), is used to refer to ‘Inherent Risk Assessment’ wheras the CIP Standards refer to a term ‘Interactive Remote Access’ but do not use an acronym. There could be confusion if an acronym is used in either document for either of these terms. We suggest not using an acronym for either term in any document. We also request clarification on why there is a specific deadline for updating the definition of LERC. As for the term ‘Low Impact External Routable Connectivity-LERC’, we suggest the drafting team edit the SAR to clarify that a revised definition will also be included in the RoP.	

When clarifying the ‘lower bound’ clarification in “adverse impact”, we would appreciate a clear example (beyond the one used in the V5TAG document) that explains this concept.

We also request the SDT review or consider creating definitions or otherwise providing clarity for ‘custom software’ and the use of ‘scripts’. There are several instances of regional inconsistencies in the scope of ‘scripts’ that should be included in an entity’s baseline. Direction or clarity from this drafting team would be appreciated. Additional requirements or definitions may not be required, but guidance, rationale, or technical background would be beneficial.

Likes 0	
Dislikes 0	

Response

Stephanie Little - 1,3,5,6

Answer	Yes
Document Name	

Comment

Arizona Public Service (AZPS) appreciates the opportunity to comment on the revised SAR, and submits the following comments previously provided in response to the initial SAR. Although AZPS generally supports the scope as described in the SAR, we believe that there are additional clarifications that should be considered beyond those detailed in the FERC Oder 822 and the CIP Version 5 Transition Advisory Group (V5TAG) considerations.

AZPS believes the industry would benefit from clarification of the definition of the following terms:

- Transmission Facility – Transmission Facility is not a defined term. Although Facility is a defined term, AZPS does not believe that the Facility definition aligns with the standard’s intent. AZPS suggests that a definition be provided by the Standard Drafting Team (SDT).
- Programmable - The SDT should consider defining programmable to clarify that a device would not be included simply because it was configurable, e.g., has functionality that can be changed locally.

AZPS would also like to suggest that the SDT clarify the intent of the grouping BCAs into BCS by leveraging the logically based perimeter security controls at the Electronic Security Perimeter (ESP) as well as local, device specific security controls per each BES Cyber Asset’s (BCA) capability.

AZPS would also like to add some additional comments to the discussion in the V5TAG CIP V5 Issues for Standard Drafting Team Consideration document.

- AZPS recommends that the SDT consider not defining “adverse impact” or defining a lower bound thereof within the definition of BES Cyber Asset, but to revise the body of CIP standards and/or applicable defined terms to utilize already defined terms such as “Adverse Reliability Impact.” Such would facilitate consistency as well as clarity regarding the N-1 contingency issue and other issues regarding that term identified by the V5TAG.
- AZPS believes that when BES Cyber Assets (BCA), such as relays, RTUs, and others, are connected via serial links to IP converters and/or IP-enabled security gateways, it would be appropriate to consider those elements downstream of the security gateways as BCA that do not have External Routable Connectivity (ERC). This is appropriate because the IP- converters and/or IP-enable security gateways require authentication and provide a protocol break. AZPS believes accurate and timely guidance related to serially connected devices supports the overall goal of providing appropriate and effective cyber security controls; thus, improving reliability.

- AZPS supports the CIP V5TAG analysis regarding virtualization. Virtualization is an effective tool for utilities and consideration should be given to ensuring that flexibility is maintained. An approach should consider the required outcome rather than the specifics of how that outcome is achieved.

AZPS also notes that NERC's webpage for this SAR "Project 2016-02 Modifications to CIP Standards", as of 4/11/2016, states the following:

"Also the scope of this work will incorporate existing and future RFIs relating to the CIP-002 through CIP-011 family of standards."

AZPS does not believe any RFIs are addressed in the current SAR. We recommend updating the SAR to reference existing submitted RFIs as appropriate. Finally, AZPS recommends removal from the SAR of functional registrations that are no longer included in the Compliance Registry, e.g., Interchange Authority, Load-Serving Entity and Purchasing-Selling Entity.

Likes 0	
Dislikes 0	

Response

Ruida Shu - 1,2,3,4,5,6,7 - NPCC, Group Name RSC

Answer	Yes
Document Name	

Comment

We support the revisions to the SAR.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

BPA agrees with the revised scope of the SAR with three exceptions regarding the "Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations –" bullet and sub-bullets:

1. BPA proposes that the SDT clearly identify which function holds the compliance documentation responsibilities.
2. BPA believes the NERC Glossary definition of control center is adequate and should not be revised. The current definition maintains the distinction between control centers and substations.
3. BPA believes no clarification of the 'performs the functions of' language is needed for Attachment 1.

Likes 0	
Dislikes 0	
Response	
larry brusseau - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darin Ferguson - 1,3,5,7 - SERC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - 10	
Answer	
Document Name	
Comment	

Texas RE supports those comments suggesting that this project should identify continued areas for improvement within the existing CIP V5 Standards and avoid engaging in a wholesale “rewrite” of the CIP Standards at this point in time. Consistent with this principle, the Standards Drafting Team (SDT) has properly identified the FERC directives from Order No. 822 and the various V5 Tag recommendations as the framework upon which to base the scope of this project.

However, Texas RE believes that the SDT should also take the opportunity to address two other areas to develop a strong record and enhance regulatory certainty around the application of the new suite of CIP Standards becoming effective on July 1, 2016. First, Texas RE agrees with those comments suggesting that the Commission should consider the interaction among the various CIP Standards, including the interaction between CIP-002-5.1 and the rest of the Standards as a group. The SDT may specifically wish to address the interplay between the various bright-line impact categories in the CIP-002-5.1 Standard and the risk assessments associated with the other CIP-005 Standards.

Second, Texas RE recommends that the SDT explicitly consider and determine whether aspects of the various supporting materials associated with the CIP Standards, including a number of Lessons Learned, FAQs, and other guidance documents should be incorporated directly into the CIP Standards themselves. For example, the October 2015 CIP V5 Consolidated FAQs and Answers provided that “HVAV, UPS, and other support systems . . . will not be the focus of compliance monitoring” unless such systems are within an Electronic Security Perimeter. (p. 7). However, some HVAC and other systems may fall within the definition of a BES Cyber System and be subject, among other things, to the categorization requirements set forth in CIP-002-5.1, R1. The SDT could add clarity to the Standards by explicitly considering whether HVAC and other support systems should be (or is already) included within the BES Cyber System definition or conversely carved out of the CIP Standards in certain circumstances. This will encourage reliability and regulatory certainty by permitting entities to look to the Standard language to understand their compliance obligations, as well as produce a transparent record of the rationale underpinning a particular approach.

Changes to SAR Redlined Language

In addition to Texas RE’s suggestions regarding the scope of this project, Texas RE also suggests two additional revisions to the revised SAR language. First, the scope of the CIP Exceptional Circumstances exception language appears vague. Texas RE presumes that the SDT incorporated the recommendations from the Edison Electric Institute and others suggesting primarily that the SDT should consider whether the CIP Exceptional Circumstances exception should be added to additional CIP V5 requirements. Texas RE recommends making this more explicit by revising the SAR language to state: “In addition, the SDT will review and address whether it is appropriate to include CIP Exceptional Circumstances exceptions within additional CIP V5 requirements.”

Second, Texas RE supports the SDT’s inclusion of language in the SAR permitting the SDT to make non-substantive changes to the Standards and Guidelines and Technical Basis sections to correct grammar, punctuation, and/or formatting errors. However, it is possible to read the proposed language to suggest that “errata” changes are somehow broader than such non-substantive revisions. Texas RE would suggest clarifying that “errata” changes to the CIP V5 Standards by inserting the word “non-substantive” in front of the word “errata” in the existing redline language.

Likes 0	
Dislikes 0	

Response

Posting Document/Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Modifications to address CIP Exceptional Circumstances

Do not use this form for submitting comments. Use the electronic form to submit comments on the modifications **to address CIP Exceptional Circumstances.** The electronic form must be submitted by **8 p.m. Eastern, March 13, 2017.**

To minimize the number of posted documents, the Standard Drafting Team (SDT) included everything in this single document with the questions following the suggested approach and draft language.

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Al McMeekin at (404) 446-9675.

Introduction

A CIP Exceptional Circumstance (CEC) is defined in the NERC Glossary of Terms Used in Reliability Standards as:

> A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

CEC are included in a Responsible Entity's cyber security policy from CIP-003 which describes how the entity would declare and respond to a CEC. During a declared CEC, the entity is allowed exception(s) to adhering to the specific reliability objective of the requirement(s); however, the entity is still compliant with the requirement(s) if the entity properly declares and responds to the CEC and adheres to its applicable cyber security policies.

From the experience and knowledge gained in the on-going efforts to implement the CIP Version 5 standards, stakeholders requested in the SAR that the CIP Modifications Standard Drafting Team (SDT) review the entire suite of CIP standards to determine whether there are any additional requirements that could be impacted during a declared CEC, and if so, to recommend revisions to those requirements. The SDT reviewed the CIP Version 5 suite of standards and identified several more instances where including the phrase "except during CIP Exceptional Circumstances" is deemed appropriate. The SDT is proposing[1] to

---

[1] The SDT previously considered a second option to handle CIP Exceptional Circumstances which required the development of a formal CEC program that allowed for a CEC to be taken for any CIP requirement, based on need. Through additional review and input, the SDT determined that any CEC declared under the framework of a holistic CEC program would require treatment under the Compliance Monitoring and Enforcement Program as an instance of potential non-compliance. Consequently, the SDT dismissed this approach and is moving forward with a proposal based on the existing CEC paradigm.

retain the existing language in the currently approved CEC-related Requirements and add the same language to additional selected Requirements/Parts as outlined below.

List of Additional Requirements for Consideration

Standard	Requirement	Rationale
CIP-004	Requirement R3, Part 3.5 Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	This is similar to the CIP-004-5 Requirement R2, Part 2.2 training requirement. A personnel risk assessment cannot be performed on first responders, and may not be possible on relevant vendors. This would cover the entity's personnel as well as contractors and service vendors
CIP-006	Requirement R1, Part 1.8 Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	This aligns to CIP-006-6 Requirement R2, Part 2.2. During certain events, logging may not be possible if the facility is damaged or destroyed.
CIP-006	Requirement R1, Part 1.9 Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	This aligns to CIP-007-6 Requirement R4, Part 4.3. During certain events, logging may not be possible if the facility is damaged or destroyed.
CIP-006	Requirement R2, Part 2.3 Retain visitor logs for at least ninety calendar days.	This aligns to CIP-007-6 Requirement R4, Part 4.3. During certain events, logging may not be possible if the facility is damaged or destroyed.
CIP-007	Requirement R4, Part 4.1 Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a	This aligns to CIP-006-6 Requirement R2, Part 2.2. During certain events, logging may not be possible if the facility is damaged or destroyed.

Standard	Requirement	Rationale
	minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	
CIP-010	Requirement R1, Part 1.4.1 Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;	This aligns to Requirement R3, Part 3.3. During the event, security controls testing may impede recovery efforts.
CIP-010	Requirement R1, Part 1.5 Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	This aligns to Requirement R3, Part 3.3. During the event, security controls testing may impede recovery efforts.

Receiving thoughtful and constructive feedback from stakeholders is critical to the success of this plan. Submitting comments in advance of the deadline is welcomed and encouraged. The SDT thanks you for your participation.

Questions

Note: The new (revised) language is shown in red text.

1. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

    CIP-004 R3, Part 3.5: Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years, except during CIP Exceptional Circumstances.

    ☐ Yes
    ☐ No

    Comments:

2. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

    CIP-006 R1, Part 1.8: Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.

    ☐ Yes
    ☐ No

    Comments:

3. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

    CIP-006 R1, Part 1.9: Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.

    ☐ Yes
    ☐ No

    Comments:

4. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-006 R2, Part 2.3: Retain visitor logs for at least ninety calendar days, except during CIP Exceptional Circumstances.

   ☐ Yes
   ☐ No

   Comments:

5. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-007 R4, Part 4.1: Log events, except during CIP Exceptional Circumstances, at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

   ☐ Yes
   ☐ No

   Comments:

6. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-010 R1, Part 1.4.1: Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change.

   ☐ Yes
   ☐ No

   Comments:

7. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

    CIP-010 R1, Part 1.5: Where technically feasible, for each change that deviates from the existing baseline configuration:

    1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected, except during CIP Exceptional Circumstances; and

    1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments, except during CIP Exceptional Circumstances.

    ☐ Yes
    ☐ No

    Comments:

8. Are there other Requirement(s) or Part(s) that should include the CIP Exceptional Circumstance language other than those already identified in this request? If so, please identify and provide the rationale.

    ☐ Yes
    ☐ No

    Comments:

9. If you have additional comments on the proposed approach that you have not provided in response to the questions above, please provide them here.

    Comments:

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

2016-02 Modifications to CIP Standards Communication Networks and CIP Exceptional Circumstances

Informal Comment Period Open through March 13, 2017

Now Available

The Project 2016-02 Standard Drafting Team (SDT) is requesting stakeholder input on two issues it is addressing: (1) the Federal Energy Regulatory Commission directive regarding Communication Networks; and, (2) determining if additional CIP requirements are impacted during a declared CIP Exceptional Circumstance. 30-day informal comment periods are open through **8 p.m. Eastern, Monday, March 13, 2017** for stakeholders to provide feedback on the SDT's approach and draft language for each issue. To minimize the number of posted documents, the SDT included everything in a single document for each issue with the suggested approach and draft language preceding the questions.

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The drafting team will review all responses received during the informal comment period and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Modifications to Address CIP Exceptional Circumstances
Comment Period Start Date:	2/10/2017
Comment Period End Date:	3/13/2017
Associated Ballots:	

There were 51 sets of responses, including comments from approximately 128 different people from approximately 97 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-004 R3, Part 3.5: Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years, except during CIP Exceptional Circumstances.

2. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R1, Part 1.8: Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.

3. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R1, Part 1.9: Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.

4. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R2, Part 2.3: Retain visitor logs for at least ninety calendar days, except during CIP Exceptional Circumstances.

5. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-007 R4, Part 4.1: Log events, except during CIP Exceptional Circumstances, at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

6. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-010 R1, Part 1.4.1: Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change.

7. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-010 R1, Part 1.5: Where technically feasible, for each change that deviates from the existing baseline configuration:

1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected, except during CIP Exceptional Circumstances; and

1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments, except during CIP Exceptional Circumstances.

8. Are there other Requirement(s) or Part(s) that should include the CIP Exceptional Circumstance language other than those already identified in this request? If so, please identify and provide the rationale.

9. If you have additional comments on the proposed approach that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Southwest Power Pool, Inc. (RTO)	Charles Yeung	2	SPP RE	SRC CIP March	Charles Yeung	SPP	2	SPP RE
					Ben Li	IESO	2	NPCC
					Mark Holman	PJM	2	RF
					Matt Goldberg	ISONE	2	NPCC
					Lori Spence	MISO	2	MRO
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC

					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC

					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO

					Chuck Lawrence	American Transmission Company	1	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Mike Buyce	City Utilities of Springfield	1,4	SPP RE
					Robert Gray	Board of Public Utilities,KS (BPU)	3	SPP RE
					Stewart Dover	Lafayette Utilities System	2	SPP RE

					John Allen	City Utilities of Springfield, Missouri	4	SPP RE
					Tara Lightner	Sunflower	1	SPP RE
Public Service Enterprise Group	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF

1. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-004 R3, Part 3.5: Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years, except during CIP Exceptional Circumstances.

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	

Comment

While the NSRF agrees with identifying those requirements impacted by CECs, we do not support revising the standards to add CEC exclusions as suggested. There is significant overhead to the Industry every time a standard is opened. It can also lead to more questions and additional standards changes to address questions raised by the Commission. There will also be additional work in the compliance arena as the RSAWS will likely ask to document all CEC events and whether they were properly assessed, or to provide proof that no CEC cases occurred.

In an effort to stabilize the CIP standards, we would recommend using NERC's new Compliance Guidance process. NERC should ask the CIPC to develop simple implementation guidance outlining how Registered Entities can document and report CECs to get Compliance Exception treatment. NERC should also draft a companion CMEP Practice Guide to enable expeditious Compliance Exception handling of access issues occurring during a CEC.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE recognizes there are instances where declaring a CIP Exceptional Circumstance (CEC) is appropriate and the Standard Drafting Team (SDT) did identify such circumstances. Given the definition of CEC, however, Texas RE recommends the SDT not extend the current application of CIP Exceptional Circumstances to the additional standards identified. The definition of CEC specifically includes situations that "involve[] or threaten[] to involve . . .an imminent or existing hardware, software, or equipment failure." That is to say, under the SDT proposal, an entity experiencing a hardware failure or system outage may declare a "CIP Exceptional Circumstance" and avoid Standard requirements that are expressly designed to encourage redundant controls and backup systems precisely in such circumstances. As a result, the proposal appears designed solely to reduce compliance risk rather than encourage sound “defense-in-depth” practices.

Consider the proposal to extend the CEC language to CIP-006 R1, P1.8, concerning the logging of physical entry into a Physical Security Perimeter. Currently, registered entities routinely accomplish this logging function through electronic devices such as card readers. However, if these devices fail, entities are expected to deploy secondary physical controls to control access. In particular, registered entities routinely post security personnel at perimeters to log entry and exit during an outage. Under the SDT’s proposal, however, such entities would no longer be required to deploy such physical personnel to log access. Rather, they could declare a CEC during the duration of the hardware failure. The net effect is to reduce the overall protections for physical assets. The same logic extend to the retention of physical access logs and visitor logs under CIP-006 R1, P1.9 and CIP-006 R2, P.2.3, respectively.

A similar rationale applies to the extension of the CEC language to the CIP-004 R3, P. 3.5 Personal Risk Assessment (PRA) requirement. In Texas RE’s experience, the best practice for entities handling the PRA process is to ensure sufficient lead-time for PRA updates and other actions. Given the seven-year review window, entities should be encouraged to perform any and all reviews with sufficient lead time so that unforeseen circumstances and events do not result in a possible violation. Again, the SDT’s proposal reduces this incentive. Critically, the SDT’s proposal applies to all entity personnel and contractors. Given the potentially broad nature of an “imminent or existing hardware, software, or equipment failure,” an entity could avoid performing background diligence on any contractor entering its facilities to perform any unscheduled, non-routine maintenance. This appears overbroad and beyond the SDT’s intent. Texas RE has identified similar issues with CIP-007 and CIP-010 listed by the SDT above.

In the alternative, Texas RE recommends the SDT revise the definition of CEC to remove “an imminent or existing hardware, software, or equipment failure”. This properly aligns the focus of the CEC definition with the rationale statements provided by the SDT for the examples above.

Texas RE also recommends clarifying entities’ compliance expectations around CECs. In particular, Texas RE has encountered a number of entities that view a CIP Exceptional Circumstances declaration as exculpatory without more. Rather, if an entity declares a CIP Exceptional Circumstance, the entity must fully document and justify the scope and duration of the event, as well as establish that regular controls were in place and appropriate elements of its emergency response plan were implemented. This proceeding is an opportunity to clarify these expectations.

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	No
Document Name	

Comment

Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2, Group Name SRC CIP March	
Answer	No
Document Name	
Comment	
While we agree with identifying those requirements impacted by CECs, we disagree with revising the standards to add CEC exclusions as suggested. There is significant overhead to the Industry every time a standard is opened. It can also lead to more questions and additional standards changes to address questions raised by the Commission. There will also be additional work in the compliance arena as the RSAWS will likely ask to document all CEC events and whether they were properly assessed, or to provide proof that no CEC cases occurred. In an effort to stabilize the CIP standards, we would recommend using NERC's new Compliance Guidance process. NERC should ask the CIPC to develop simple Implementation Guidance outlining how Registered Entities can document and report CECs to get Compliance Exception treatment. NERC should also draft a companion CMEP Practice Guide to enable expeditious Compliance Exception handling of access issues occurring during a CEC.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP agrees personnel risk assessments can’t be performed on first responders and some relevant vendors.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

It is impractical to refuse entry to an emergency responder or SME due to the lack of a PRA or have to wait to validate a PRA. This would potentially hinder recovery/response efforts.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO

Answer	Yes
Document Name	

Comment

CIP Exceptional Circumstance was approved for this requirement in previous versions. If there is an emergency situation as described by the definition of a CIP Exceptional Circumstance, there isn’t time to get a background check completed before allowing rescue/medical personnel in to assist.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

AZPS respectfully requests that the addition of the existing CIP Exceptional Circumstance language be applied to CIP-004 R3, Parts 3.1 through 3.5 and be placed at the beginning of the opening phrase. AZPS believes that the performance of all Parts under Requirement R3 would not be feasible during a CIP Exceptional Circumstance, e.g., companies would not seek to confirm the identity of paramedics responding to the medical emergency of an employee.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement parts. Specifically, it is important to highlight that for CIP-004-5, R3, the Personnel Risk Assessments (PRA) may not be able to be performed on first responders, whether they are entity personnel or external contractors, vendors or emergency personnel, within a reasonable period of time prior to authorizing unescorted physical access during a CIP exceptional circumstance.

CIP Exceptional Circumstances are declared in emergency situations to protect life, safety and the reliability of the BES. Entities are given the flexibility to design programs that articulate how to declare and respond to a CEC. That flexibility should extend to the entity’s ability to appoint or allow individuals with appropriate skills to assist with recovery to gain access as necessary to mitigate risk.

Additionally, during a major BES Cyber System event there may be a need to provide access to the vendor to address the system issue where obtaining a PRA for electronic access would prohibit addressing maintaining reliability. The seven (7) year criminal history checks may may require searches across multiple jurisdictions for a single individual based on resident history. Jurisdications are not required to respond to requests for criminal history information within a specified service level agreement (SLA). In addition, some jurisdications require fingerprinting or other means to authenticate the criminal history of an individual, which would extend the amount of time required to complete the PRA.

Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Recommend changing the order of the wording to: "Process to ensure, except during CIP Exceptional Circumstances, that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years."	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Requirement 3 of CIP-004-6 Guidelines and Technical Basis already referenced CEC:"Each Responsible Entity shall ensure a personnel risk assessment … except for program specified exceptional circumstances". Can a requirement be suspended for CEC even if it does not allow CEC explicitly? What if the G&TB makes a reference to CEC but not the requirement? What should be the procedure for reporting the CEC in a case where CEC is not explicitly mentioned in the requirement?	
Likes 0	
Dislikes 0	
Response	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
As noted in the rationale, this is consistent with CIP-004 R2, Part 2.2. This exception is needed to address instances where first responders or others providing assistance in a CEC require access. In the event of a CEC, obtaining a personnel risk assessment prior to allowing access may cause risk to life or property. Additionally, in the event of a CEC, obtaining a PRA for vendors involved with restoration may not be practical. ERCOT also suggests the SDT consider revising the language to further clarify that the exception applies to the need to conduct a PRA, and not to the period covered by the PRA. This could be addressed as follows: "Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years. The requirement to complete a personnel risk assessment does not apply during CIP Exceptional Circumstances."	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Agree with SDT rationale	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes

Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-004 R3, Part 3.5. Compliance with this requirement should not hinder first responders efforts to respond to emergency situations.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
During CEC the process is it not feasible to ensure individals with authorized electronic or authorized unescorted physical access have a personnel risk assessment completed.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
To provide consistency between the two major pre-requisites contained within CIP-004-6 R2 (Training) and CIP-004-6 R3 (PRA), the CEC langauge could be added where if Training is not required during a CEC prior to allowing emergency access, the requirements for R3 should allow for the same. Additionally, it could also be considered that CEC exemptions under R2 and R3 are not necessary based on the CEC exemption under CIP-004-6 R4.1, which allows an Entity to forego "authorizing access based on need" during a CEC. For example - if emergency responders are responding to a fire in a PSP, there would be no intention to "authorize" those personnel for unescorted access (which would require background checks and training) because they would be considered visitors, and the exemption under CIP-004-6 R4.1 should be sufficient. CIP-006-6 R2 also allows a CEC exemption to allow an Entity to forego escorting and logging visitors into a PSP during a CEC.	
Likes 0	

Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R1, Part 1.8: Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	

Southern supports the inclusion of a CEC exemption under R1.8, but also provides the following for consideration under CIP-006: Under CIP-006-6 R1.4 and R1.6 – ‘Monitor for unauthorized access’ is a requirement where your ability to monitor constantly, 24x7, may be impacted by the onset of a CEC. For example – if a tornado or flood renders your ability to perform 24x7 monitoring unavailable until you can dispatch personnel or implement alternative means of monitoring – are you in violation of not performing 24x7 monitoring during the period you are convening and dispatching personnel to perform human observation and monitoring? What if, due to flooding, the PSP access points (or PACS assets) are inaccessible and monitoring communications circuits are down – removing your ability to dispatch personnel? Shouldn’t R1.4 and R1.6 provide the ability to respond to and address monitoring when it has been impacted by a CEC? Similarly, if you are unable to monitor due to the onset of a CEC, you are likely also unable to issue an alarm or alert during that CEC. Consider, under CIP-006-6 R1.5 and 1.7 – ‘Issue an alert in response to detected unauthorized access,’ should be included as requirements that need a CEC exemption; otherwsie, are you in violation if a tornado or flood has taken out your standard implementation of alarm issuance during the period you are implementing back-up measures?	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SCE agrees with the rationale provided during a CEC.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-006 R1, Part 1.8. AECI agrees with the SDT's assertion that during certain events, logging may not be possible if the facility is damaged or destroyed.	
Likes 0	

Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Agree with SDT rationale although it is harder to envision a scenario where we wouldn't want to log entry of authorized personnel in some manner, even someone with a clipboard taking notes.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
As noted in the rationale, this aligns to CIP-006 R2, Part 2.2. During certain events, logging may not be possible if the facility is damaged or destroyed.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
This makes the requirement consistent with that for visitors in Part 2.2. However, I believe some measure of control is needed to ensure that, even during CIP Exceptional Circumstances, carte blanche access is not provided to all. This provides a potential secondary attack vector to those who	

otherwise might not have access. While perhaps full-fledged logging may not be required, some access list verification (including "approved visitors" needed for addressing the emergency is required.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Exelon supports the addition of "except during CIP Exceptional Circumstance" to the Requirement part. Authorized unescorted physical access is logged automatically, or manually in the event that the automated system is unavailable. If a facility is damaged or destroyed, it may not be possible to control access via the automated system. Having resources to manually log individuals with authorized unescorted physical access to PSPs during a declared CEC may compromise the safety of the personnel logging access. Additionally, the amount of time to manually log entry could hinder recovery efforts resulting in increased risk to the BES. CIP Exceptional Circumstances are declared in emergency situations to protect life, safety and the reliability of the BES. Entities are given the flexibility to design programs that articulate how to declare and respond to a CEC. That flexibility should extend to the entity's ability to appoint or allow individuals with appropriate skills to assist with recovery to gain physical access as necessary to mitigate reliability risks.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
Under some circumstances when a CIP Exception Circumstance is allowed, it may or may not be possible to capture log this information manually. Entities should do their best, but CIP Exceptional Circumstance will still be needed in some of the possible scenarios.	
Likes 0	
Dislikes 0	

Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Depending on the nature of the incident, the RE makes every effort to maintain logs of physical attendance; however, this process should not hinder recovery/response efforts.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees that logging may not be possible if facility is damaged or destroyed.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	

Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s comments in response to #1.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
See comments on Question No. 1	
Likes 0	
Dislikes 0	
Response	

3. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language. **CIP-006 R1, Part 1.9: Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.**

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Because logging may not be occurring during a CIP Exceptional Cirumstance, there may be no logs to actually retain pursuant to this requirement. Further, if logging is ocurring, there is no need for a CIP Exceptional Circumstance to be applied to the log retention requirements. Thus, AZPS recommends that, relative to retention requirements, the phrase 'except during a CIP Exceptional Circumstance' be modified to state 'except if such logs are adversely impacted or destroyed as a result of a CIP Exceptional Circumstance'.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	No
Document Name	
Comment	
The rationale that is listed is not valid for this requirement. While I agree that logging may not be possible during periods when the facility is damaged and destroyed, it's not that logging can't be perfromed. It's that the log repository may be destroyed and rendered unusable.	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	

Comment	
Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees that logging may not be possible if facility is damaged or destroyed.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes

Document Name	

Comment

Depending on the nature of the incident, the RE should make every reasonable effort to maintain logs of physical attendance; however, this process should not hinder recovery/response efforts.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO

Answer	Yes
Document Name	

Comment

If a log is not created as required by Part 1.8 due to CIP Exceptional Circumstance, it logically follows that it won’t be possible to retain it due to CIP Exceptional Circumstance.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement part. As discussed in the response to question 2, it was noted that logging of authorized unescorted physical access could increase risks to personal safety and the reliability of the BES. During CECs where logging is not possible or practical, logs would not exist to retain for 90 days. Further, It is understood that for CECs where logging of authorized unescorted physical access took place, the entity would adhere to the 90 day retention requirement to the best of its ability. There may be situations where databases or manual records have gaps despite the fact that authorized unescorted physical access was granted as a result of the circumstances pertaining to the declared CEC. Additionally, where automation is used to record and retain the historical records of physical access logs, depending on the circumstances of the declared CEC, it is possible those records could have been partially or completely lost due to events of the declared CEC.

Exelon recommends that the SDT add language to the Guidelines and Technical Basis that provide brief discussion about examples of scenarios where the ability to retain physical access logs for 90 days may not be possible as a result of a declared CEC.	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
What if the physical access logs are damaged during a CEC, should they still be retained?	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes this aligns with 1.8.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment	
As noted in the rationale, this aligns to CIP-007-6 R4, Part 4.3. During certain events, logging may not be possible if the facility is damaged or destroyed. If the events are not logged due to a failure of CIP-006 R1, Part 1.8, the logs cannot be retained for ninety calendar days. Also, the current phrasing of the exception could suggest that the retention obligation does not apply during a CEC; however, ERCOT assumes the intent of the exception is that there should be no obligation to retain information that wasn't logged in the first place due to a CEC, consistent with the exception in part 1.8. In keeping with this purpose, ERCOT suggests modifying the sentence as follows: "…for at least ninety calendar days, except for any entry that was not logged due to a CIP Exceptional Circumstance."	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
In cases were we don't log (Part 1.8) or logs are destroyed, it is impossible to retain what we don't have.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-006 R1, Part 1.9. As stated in the AECI's previous response, during certain events, logging may not be possible if the facility is damaged or destroyed.	
Likes 0	

Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SCE agrees with the rationale provided during a CEC if the system storing the logs is impacted.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
As an extension to the justification under CIP-006-6 R1.8, if due to a CEC you are unable to log, you are also unable to retain logs that don't exist. Therefore, to provide consistency with the proposed modifications under R1.8, a CEC exemption should be added to R1.9 as well.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
See comments on Question No. 1	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s comments in response to #1.	
Likes 0	
Dislikes 0	
Response	

4. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R2, Part 2.3: Retain visitor logs for at least ninety calendar days, except during CIP Exceptional Circumstances.

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	No
Document Name	

Comment

Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Essential Power, LLC - 5

Answer	No
Document Name	

Comment

The rationale that is listed is not valid for this requirement. While I agree that logging may not be possible during periods when the facility is damaged and destroyed, it's not that logging can't be perfromed. It's that the log repository (in this case, perhaps the manual visitor log book) may be destroyed and otherwise unreadable.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment	
Because logging may not be occurring during a CIP Exceptional Cirumstance, there may be no logs to actually retain pursuant to this requirement. Further, if logging is ocurring, there is no need for a CIP Exceptional Circumstance to be applied to the log retention requirements. Thus, AZPS recommends that, relative to retention requirements, the phrase ‘except during a CIP Exceptional Circumstance’ be modified to state ‘except if such logs are adversely impacted or destroyed as a result of a CIP Exceptional Circumstance’	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
As an extension to the justification under CIP-006-6 R1.8 and R1.9, if due to a CEC you are unable to log, you are also unable to retain logs that don't exist. Therefore, to provide consistency with the proposed modifications under R1.8 and R1.9, a CEC exemption should be added to R2.3 as well.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
SCE agrees with the rationale provided during a CEC.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-006 R2, Part 2.3. During certain events, logging may not be possible if the facility is damaged or destroyed.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Again, if logs are destroyed, can't retain.	
Likes 0	
Dislikes 0	
Response	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
As noted in the rationale, this aligns to CIP-007-6 R4, Part 4.3. During certain events, logging may not be possible if the facility is damaged or destroyed. If the events are not logged due to a failure of CIP-006 R2, Part 2.2, the logs cannot be retained for ninety calendar days. Also, ERCOT notes that the current exception language could be read to apply to the duration of retention, and not to the underlying obligation to retain visitor logs that weren't created in the first place due to a CEC. ERCOT therefore suggests that the SDT consider the following clarification: "…for at least ninety calendar days, except for any visitor entry that was not logged due to a CIP Exceptional Circumstance."	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
What if the physical access logs are damaged during a CEC, should they still be retained?	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement part. Vistors are manually logged by site personnel. Manually logging individuals who are visitors during CECs may compromise the safety of the personnel logging access. Additionally, the amount of time to manually log entry could hinder recovery efforts resulting in increased risk to the BES.

CIP Exceptional Circumstances are declared in emergency situations to protect life, safety and the reliability of the BES. Entities are given the flexibility to design programs that articulate how to declare and respond to a CEC. That flexibility should extend to the entity’s ability to appoint or allow individuals with appropriate skills to assist with recovery to gain access as necessary to mitigate risk.

Just as with the physical access log retention, there may be situations where databases or manual records have gaps despite the fact that physical access for visitors was granted. Additionally, where automation is used to record and retain the historical records of physical access logs for visitors, depending on the circumstances of the declared CEC, it is possible those records could have been partially or completely lost as a result of the events pertaining to the declared CEC event.

Exelon recommends that the SDT add language to the Guidelines and Technical Basis that provide brief discussion about examples of scenarios where the ability to retain physical access logs for visitors for 90 days may not be possible as a result of a declared CEC.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO

Answer	Yes
Document Name	

Comment

CIP Exceptional Circumstances exists for CIP-006 R2, Part 2.2 regarding logging visitors. It logically follows that it won’t be possible to retain visitor logs if they weren’t created due to CIP

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

Depending on the nature of the incident, the RE should make every reasonable effort to maintain logs of physical attendance; however, this process should not hinder recovery/response efforts.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees that logging may not be possible if facility is damaged or destroyed.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s comments in response to #1.	
Likes 0	
Dislikes 0	
Response	

5. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-007 R4, Part 4.1: Log events, except during CIP Exceptional Circumstances, at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
By stating “per BES Cyber Asset/System capability” this additional language does not seem necessary. In the event of an exceptional circumstance that causes damage to a device, it would seem reasonable to assume that capability is not present during that time period.	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees that logging may not be possible if facility is damaged or destroyed.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Depending on the nature of the event and/or condition of the cyber asset collecting the logs, log events may not be available. CIP Exceptional Circumstance language would then apply.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	

Comment	
Logging events may not be possible due to equipment failure.	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS respectfully submits that the complex software and tool sets utilized to log events for malicious code may also be utilized to generate alerting for such events. Therefore, if such software and tool sets are impacted during a CIP Exceptional Circumstance and are unable to log, they may also be unable to generate alerts. Accordingly, we recommend the addition of the existing CIP Exceptional Circumstance language to Part 4.2.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement part. Event logging at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) may not be possible during certain CECs if a facility is damaged or destroyed. For some operational technology devices where a replacement device is a new device type, it may be necessary to develop custom log parsing settings in order to obtain and import the logs to an automated log management solution as a result of the declared CEC.	
Likes 0	
Dislikes 0	
Response	

Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
If the device is destroyed due to hardware failure, fire, water damage, or other, and the only logging capability is local to the device, the entity should be able to follow their CIP Exceptional Circumstances process. This might be the case for devices that are serial only and do not have the capability/connections to send logs to a SIEM tool.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
The circumstances associated with the declaration of CIP Exceptional Circumstances may have damaged or destroyed monitoring and logging systems such that event logs cannot be retained.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-007 R4, Part 4.1. During certain events, logging may not be possible if the facility is damaged or destroyed.	

Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SCE agrees with the rationale provided during a CEC.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s comments in response to #1.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
As noted in the rationale, this aligns to CIP-006 R2, Part 2.2. During certain events, logging may not be possible if the facility is damaged or destroyed.	
Likes 0	
Dislikes 0	

Response

6. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-010 R1, Part 1.4.1: Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change.

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO

Answer	No
Document Name	

Comment

During CIP Exceptional Circumstance (CEC), in the interest of restoring the BES, there may not be time to determine required cyber security controls that may be impacted by the change. If this is done, due to CEC, then it logically follows that CIP Exceptional Circumstances should be applied to all parts of CIP-010 R1, Part 1.4 because they are tied together. Therefore, add the phrase at the Part 1.4 level. For example, “Except during CIP Exceptional Circumstances, for a change that deviates from the existing baseline configuration: 1.4.1……, 1.4.2…… and 1.4.3……”

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	Yes
Document Name	

Comment

All of CIP-010-2 R1 should allow for CEC exemption. CIP-010-2 R1 and each of its sub-requirements all constitute "documentation" exercises that, when responsing to a CEC, may be required to be postponed or would be considered secondary to restoring power. Without similar caveats that are found in R1.3 allowing for documentation updates to be completed within 30 days, a CEC exemption is necessary for R1.1, R1.2, R1.4, and R1.5 when commissioning new devices needed in responding to a CEC.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
From an industry perspective, SCE agrees.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-0010 R1, Part 1.4.1. During a CEC event, cyber security control testing may hinder the Responsible Entitiy's recovery efforts.	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
The "return to normal operations" following CIP Exceptional Circumstances should include a validation that appropriate controls have not been impacted. Requiring this effort during CIP Exceptional Circumstances does not appear to add value and may impede restoration efforts.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
As noted in the rationale, this aligns to R3, Part 3.3. During the event, security controls testing may impede recovery efforts. Security controls should be examined on the production system following the conclusion of the declared CEC.	
Likes 0	
Dislikes 0	

Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Agree in concept but judgment still needs to be applied to verify the intended outcome is achieved without compromising security controls. Perhaps the verification of controls occurs after the emergency has ended and the facility and/or assets is again functioning in a normal capacity.	
Likes 0	
Dislikes 0	
Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
In the event of a CEC such as a natural disaster (hurricane/tornado) or an event that requied mutual assistance for restoration, an entity might need to rebuild/restore equipment without documenting the potential changes to cyber security controls. The restoration of the BES functionality in a safe and secure manner would be first priority. Security controls could be verified after the fact to ensure that appropriate controls are in place.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement part. Entity change controls require a rigorous approval and testing process for changes to a BES Cyber Asset or BES Cyber System. In the event of a CEC, existing processes may not afford enough flexibility to conduct recovery in a way that rapidly mitigates the risk to the reliability of the BES.	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS respectfully asserts that the entirety of Requirement R1.4 is what comprises security control testing, and, as such, recommends the addition of the CIP Exceptional Circumstances language to the opening phrase of Requirement R1.4.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Depending on the nature of the incident, the RE should make every reasonable effort to determine impacted cyber security controls; however, this process should not hinder recovery/response efforts.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
SRP agrees that during a CIP Exceptional Circumstance, security controls testing may impede recovery efforts.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment	
Please see Texas RE’s comments in response to #1.	
Likes 0	
Dislikes 0	
Response	

7. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-010 R1, Part 1.5: Where technically feasible, for each change that deviates from the existing baseline configuration:

1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected, except during CIP Exceptional Circumstances; and

1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments, except during CIP Exceptional Circumstances.

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees that during a CIP Exceptional Circumstance, security controls testing may impede recovery efforts.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	
Comment	
Depending on the nature of the incident, the RE should make every reasonable effort to test changes in a test environment; however, this should not hinder recovery/response efforts.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	Yes
Document Name	
Comment	
If CEC is used for CIP-010 R1, Part 1.4, it logically follows that CEC should be allowed for testing the changes. The wording works, but the CEC phrase could be added only once at the CIP-010 R1 Part 1.5 level to cover both sub-parts with one phrase.	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS respectfully asserts that the entirety of Requirement R1.5 should be subject to CIP Exceptional Circumstances. Accordingly, AZPS recommends that the addition of the CIP Exceptional Circumstances language to the opening phrase of Requirement R1.5.	
Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Exelon supports the addition of “except during CIP Exceptional Circumstance” to the Requirement part. Entity change controls require a rigorous approval and testing process for changes to a BES Cyber Asset or BES Cyber System. In the event of a CEC, existing processes may not afford enough flexibility to conduct recovery in a way that rapidly mitigates the risk to the reliability of the BES.

For clarity, Exelon suggests moving the “except during CIP Exceptional Circumstances” phrase closer to the front of 1.5.1 and 1.5.2 as noted below. This ensures that the phrase applies to the entire Requirement Part, and not just the last clause of the text.

1.5.1. Prior to implementing any change in the production environment, **except during CIP Exceptional Circumstances,** test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and

1.5.2. Except during CIP Exceptional Circumstances, document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Likes 0	
Dislikes 0	

Response

Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC

Answer	Yes
Document Name	

Comment

In the event of a CEC such as a natural disaster (hurricane/tornado) or an event that requied mutual assistance for restoration, an entity might need to rebuild/restore equipment without testing cyber security controls and documenting the test. The restoration of the BES functionality in a safe and secure manner would be first priority. Security controls could be verified after the fact to ensure that appropriate controls are in place.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Agree in concept but judgment still needs to be applied to verify the intended outcome is achieved without compromising security controls. Perhaps the verification of controls occurs after the emergency has ended and the facility and/or assets is again functioning in a normal capacity.	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Are there other Requirement(s) or Part(s) that should include the CIP Exceptional Circumstance language other than those already identified in this request? If so, please identify and provide the rationale.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
As noted in the rationale, this aligns to R3, Part 3.3. During the event, security controls testing may impede recovery efforts. Security controls should be examined on the production system following the conclusion of the declared CEC.	

ERCOT also suggests moving the exception to the beginning of the language, as follows:

1.5.1 Except during a CIP Exceptional Circumstance, and prior to implementing any change in the production environment…”

And

“1.5.2 Except during a CIP Exceptional Circumstance, document the results of the testing…”

Likes 0	
Dislikes 0	

Response

Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF

Answer	Yes
Document Name	

Comment

Having the exceptional circumstances language in both subparts ensures that there is no question whether it is applicable to both subparts.

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	Yes
Document Name	

Comment

Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.

Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees with adding the existing CIP Exceptional Circumstance language to CIP-010 R1, Part 1.5.1 and 1.5.2. During a CEC event, cyber security control testing may hinder the Responsible Entitiy's recovery efforts.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
We agree with the rationale provided during a CEC.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	

All of CIP-010-2 R1 should allow for CEC exemption. CIP-010-2 R1 and each of its sub-requirements all constitute "documentation" exercises that, when responsing to a CEC, may be required to be postponed or would be considered secondary to restoring power. Without similar caveats that are found in R1.3 allowing for documentation updates to be completed within 30 days, a CEC exemption is necessary for R1.1, R1.2, R1.4, and R1.5 when commissioning new devices needed in responding to a CEC.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's comments in response to #1.	
Likes 0	
Dislikes 0	
Response	

8. Are there other Requirement(s) or Part(s) that should include the CIP Exceptional Circumstance language other than those already identified in this request? If so, please identify and provide the rationale.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
Include the electronic and physical security controls required by CIP-003 R2 Attachment 1, sections 2 and 3. This would meet the same rational as used for the inclusion of CEC for CIP-004 and CIP-006.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	No
Document Name	
Comment	
No additional requirements identified as applicable.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
Likes 4	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey; PSEG - PSEG Energy Resources and Trade LLC, 6, Jara Karla
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3 - MRO	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	

When considering Requirements against the elements of the CEC Definition, the view often focuses on time limited events measured in minutes, hours, or a day. We encourage a wider view. For example: An impediment of large scale workforce availability conceivably affects Requirements with time periods of multiple days, weeks, even months. This view stems from an entity's priority of operating the BES which may replace its ability to complete administrative efforts dedicated to program updates—while important—they fall out of the active operation of the BES to maintain reliability in emergency circumstances.

It is in consideration of this type of scenario we offer the following additional Requirements:

Rationale: Difficult to Adhere to Short Time-Based Requirements if During A CEC:

CIP-004-6 R5.1 (24-hour termination);

CIP-004-6 R5.3 (1-day termination to CII Repository);

CIP-004-6 R5.4 (30-day termination to shared accounts);

CIP-007-6 R2.2 (35-day patch evaluation);

CIP-007-6 R2.3 (35-day patch implementation/mitigation);

CIP-007-6 R4.4 (15-day logged event review);

CIP-010-2 R1.3 (30-day baseline configuration update after the change);

CIP-010-2 R2.1 (35-day baseline configuration monitoring);

Rationale: Similar Rationale As Other Requirements Added By SDT FOR CIP-010 R1, Part 1.4.1: CIP-010-2 R1.2 (authorize & document changes that deviate from the baseline configuration); Rationale: Similar Rationale As Other Requirements Added By SDT FOR CIP-007-4: CIP-007-6 R4.2 (security event alerting); CIP-004-6 R4.2 (quarterly access review) depending on timing of CEC.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Please see above responses where reference to additional requirements for consideration have been addressed.	
Likes 0	
Dislikes 0	
Response	

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Any requirement that requires real-time or near real-time alerting and response should include the CEC phrase. For example, CIP-004 R5, that addresses access revocations. In the case of CEC, response to a termination action or reassignment could be significantly delayed.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
CIP-004-6, R5, Part 5.1 - The Responsible Entity may not be able to remove an individual's ability for unescorted physical access and Interactive Remote Access if an asset is damaged or destroyed during a CEC. CIP-006-6, R1, Parts 1.2 – 1.7, & 1.10 – During a CEC, Physical Access Control Systems may be damaged or destroyed, preventing the Responsible Entity from strict adherence to these requirements. CIP-007-6, R4 Part 4.2 - The Responsible Entity may not be able to generate alerts for applicable security events if logging is not functional in accordance with CIP-007-6 R4 Part 4.1. CIP-007-6, R4 Part 4.4 – During a CEC, logging may not be functional if the facility is damaged or destroyed. CIP-010-2 R1, Parts 1.1 – 1.3 – Change management controls may impede recovery efforts during a CEC.	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per standard/requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	Yes
Document Name	
Comment	
All standards, requirements, and parts related to reliability and safety should include the CIP Exceptional Circumstance language.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - RES Americas Inc. - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Yes- if a facility is significantly damanged or destroyed all CIP requrements and sub requirements should be considered for CEC. For Example, Update of the Recovery Plan required by CIP-009-5 R3, Part 3.1 if the CEC lasts for more than 90 days.	

Update of the CIP Cyber Asset list required by CIP-002.

Testing of the recovery plan required by CIP-009-5 R2 Part 2.3 if the CEC is occurring during the planned testing date.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	Yes
Document Name	

Comment

- CIP-004-6 R5.1 Consider – In the case of a CEC, it may not be possible to complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights). The ability to remove access may be impeded because of an event triggering a CIP exceptional circumstance.

- CIP-005-6 R1.1 Consider – In the case of a CEC, all applicable Cyber Assets connected to a network via a routable protocol may not reside within a defined ESP.

ESP might not be defined in the case that the network, including Cyber Assets connected via a routable protocol, has to be rebuilt because of an event triggering a CIP exceptional circumstance.

- CIP-005-6 R1.3 Consider – In the case of a CEC, it may not be possible to have inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. Access permissions might not be defined in the case that the network, including Cyber Assets connected via a routable protocol, has to be rebuilt because of an event triggering a CIP exceptional circumstance.

- CIP-005-6 R1.4 Consider – In the case of a CEC, it may not be possible to perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets. Performing authentication, when establishing Dial-up Connectivity with applicable Cyber Assets, might not be possible in the case that the network, including Cyber Assets connected via a routable protocol, has to be rebuilt because of an event triggering a CIP exceptional circumstance.

- CIP-005-6 R1.5 Consider – In the case of a CEC, it may not be possible to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. Having a method for detecting known or suspected malicious communications for both inbound and outbound communications, might not be possible in the case that the network, including Cyber Assets connected via a routable protocol, has to be rebuilt because of an event triggering a CIP exceptional circumstance.

- CIP-006-6 R1.2 Consider – In the case of a CEC, it may not be possible to utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access. In the event of a failure of a PACS, it may not be possible to have 1 factor for access control.

- CIP-006-6 R1.3 Consider – In the case of a CEC, it may not be possible to utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access. In the event of a failure of a PACS, it may not be possible to have two factor access controls.

- CIP-006-6 R1.4 Consider – Monitoring unauthorized access through a physical access point into a Physical Security Perimeter may not be possible in the case that the logging and/or monitoring system is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-006-6 R1.5 Consider – Issuing an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection may not be possible in the case that the logging and/or monitoring system, required to detected unauthorized access, is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-006-6 R1.6 Consider – Monitoring each Physical Access Control System for unauthorized physical access to a Physical Access Control System may not be possible in the case that the logging and/or monitoring system, required to monitor unauthorized physical access to PACS, is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-006-6 R1.7 Consider – Issuing an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection may not be possible in the case that the logging and/or monitoring system, required to detected unauthorized access to PCAS, is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-007-6 R2.3 Consider – It may not be possible to apply applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, if the asset to be patched is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-007-6 R4.2 Consider – Generating alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, to detected malicious code from Part 4.1 and detected failure of Part 4.1 event logging, may not be possible in the case that the system to detect malicious code and/or the system required to detect event logging failure, is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-007-6 R4.4 Consider – Reviewing a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents, may not be possible in the case that the system required to log events, is damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-008-5 R2.1 Consider – It may not be possible to test each Cyber Security Incident response plan(s) at least once every 15 calendar months, by responding to an actual Reportable Cyber Security Incident, with a paper drill or tabletop exercise of a Reportable Cyber Security Incident or with an operational exercise of a reportable Cyber Security Incident. The ability to test the plan may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoke for that requirement in the case of a Cyber Security incident that mobilize the same staff required to test the Cyber Security response plan)

- CIP-008-5 R2.3 Consider – It may not be possible to retain records related to Reportable Cyber Security Incidents in the case that the records are damaged or destroyed because of an event triggering a CIP exceptional circumstance.

- CIP-008-5 R3.1 Consider – No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response, it may not be possible to document any lessons learned or document the absence of any lessons learned, to update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan and to notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned. The ability to document any lessons learned, update the plan and notify each person may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoked for that requirement in the case of a general strike)

- CIP-008-5 R3.2 Consider – No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan, it may not be possible to update the Cyber Security Incident response plan(s) and notify each person or group with a defined role in the Cyber Security Incident response plan of the updates. The ability to update the plan and notify each person may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoked for that requirement in the case of a general strike)

- CIP-009-6 R2.1 Consider – It may not be possible to test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months, by recovering from an actual incident, with a paper drill or tabletop exercise or with an operational exercise. The ability to test the recovery plan may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoked for that requirement in the case of a general strike)

- CIP-009-6 R2.2 Consider – It may not be possible to test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. The ability to test a representative sample of information used to recover BES Cyber System functionality may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoked for that requirement in the case of a general strike).

- CIP-009-6 R2.3 Consider – It may not be possible to test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. The ability to test the recovery plans may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoked for that requirement in the case of a general strike).

- CIP-009-6 R3.1 Consider – No later than 90 calendar days after completion of a recovery plan test or actual recovery, it may not be possible to document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned, to update the recovery plan based on any documented lessons learned associated with the plan and to notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned. The ability to document any lessons learned, update the recovery plan and notify each person may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoke for that requirement in the case of a general strike)

- CIP-009-6 R3.2 Consider – No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan, it may not be possible to update the recovery plan and notify each person or group with a defined role in the recovery plan of the updates. The ability to update the recovery plan and notify each person may be impeded because of an event triggering a CIP exceptional circumstance. (Example: a CEC could be invoke for that requirement in the case of a general strike)

- CIP-011-1 R2.1 Consider – Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), it may not be possible that the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media in the case that the applicable Cyber Asset is no longer available because of an event triggering a CIP exceptional circumstance. (Example: A Cyber Asset containing BES Cyber System Information was stolen during a physical intrusion by terrorist)

- CIP-011-1 R2.2 Consider – Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, it may not be possible that the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media in the case that the applicable Cyber Asset or the data storage media is no longer available because of an event triggering a CIP exceptional circumstance. (Example: A Cyber Assets containing BES Cyber System Information was stolen during a physical intrusion by terrorist)

- Attachment 1, Section 2 (Physical Security Controls for low impact)

Consider – Control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any, may not be possible in the case that the physical control in place is damaged or destroyed because of an event triggering a CIP exceptional circumstance. (Example: emergency services destroyed physical lock that controls access in order to give assistance)

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Include the electronic and physical security controls required by CIP-003 R2 Attachment 1, sections 2 and 3. This would meet the same rational as used for the inclusion of CEC for CIP-004 and CIP-006.	
Likes 0	
Dislikes 0	
Response	
Adam Padgett - TECO - Tampa Electric Co. - 1,3,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
CIP-003-6 Attachment 1 Section 2 should have the CIP Exceptional Circumstance language for physical security relative to the clause “shall control physical access, based on need.” While an entity could use language in their CIP-003 R2 Attachment 1 Section 2 to indicate that first responders have a “need,” it would be preferable to use the same program used for CIP-006 for consistency across all locations.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes

Document Name	
Comment	

IPC would like the following CIP requirements added to the CEC list of requirements:

CIP-005-5 R1, Parts R1.1 to R1.5—There may be times during a CEC when a Responsible Entity will be in a position where holding their ESP intact is not feasible, possible, or will extend an operational outage or issue creating additional reliability concerns. A Responsible Entity should be provided with a high degree of latitude to address a CEC and be provided the tools necessary to address reliability concerns without concurrent compliance concerns.

CIP-006-6 R1, Parts R1.2 to R1.7—Although it is ideal to maintain Parts R1.2 to R1.7 in every circumstance, during a CEC, it may not be feasible for a Responsible Entity to utilize two-factor access controls, monitor physical access points, or issue alarms. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-007-6 R1, Parts R1.1 & R1.2—Although it is ideal to maintain Parts R1.1 and R1.2 in every circumstance, during a CEC, a Responsible Entity may not have time to document and protect every port. While port security is important, a Responsible Entity should have the flexibility to document and protect the applicable ports when the CEC has been corrected. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-007-6 R4, Part 4.2—If logging is unavailable due to a CEC for CIP-007-6 Part 4.1, generating alerts for security events for Part 4.1 would most likely be unavailable as well. A Responsible Entity should be given the flexibility to determine what they are able to keep in place based on the event taking place and suspend those requirements that are either ineffective or non-functioning based on the situation.

CIP-007-6 R4, Part 4.4—If logging is unavailable due to a CEC for CIP-007-6 Part 4.1, reviewing logs would not be possible for the time the logging system is down during the CEC, which may exceed 15 calendar days.

CIP-007-6 R5, Parts R5.1 to R5.3—Although it is ideal to maintain Parts R5.1 to R5.3 in every circumstance, during a CEC, a Responsible Entity may not have time to identify and enforce certain system access controls. While authentication, inventories of all generic accounts, and lists of those who can access shared accounts is important, it may not be necessary to have this documentation updated during a CEC where new devices are being implemented or old devices are being wiped and rebuilt. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-010-2 R1, Parts 1.1 to R1.4, including R1.4.2 & R1.4.3—Change management is a critical piece of day-to-day operations to maintain good process controls and practices. However, rigid change management processes and baseline documentation could just as easily be a hindrance to recovery efforts during a CEC. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-010-2, Attachment 1, Section 1.1 to 1.5—Although it is ideal to maintain Sections 1.1 to 1.5 in every circumstance, during a CEC, it may not feasible for a Responsible Entity to use only those devices that are designated as a TCA. Some instances may require additional resources from within a Responsible Entity that would not be approved TCAs. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning

CIP-010-2, Attachment 1, Section 2.1 to 2.3—Although it is ideal to maintain Sections 2.1 to 2.3 in every circumstance, during a CEC, it may not be feasible for a Resonsible Entity to mitigate software vulnerabilities and malicious code for TCAs managed by a party other that the Responsible Entity. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-010-2, Attachment 1, Section 3.1 to 3.2—Although it is ideal to maintain Sections 3.1 to 3.2 in every circumstance, during a CEC, it may not be feasible for a Responsible Entity to use only those devices that are designated as a RM. Some instances may require additional resources from within a

Responsible Entity that would not be approved RM. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

CIP-011-2 R1, Part R1.2—Although it is ideal to maintain Part R1.2 in every circumstance, during a CEC, it may not be feasible for a Responsible Entity to maintain adherence to a Responsible Entity's Information Protection Program. A Responsible Entity should have the flexibility to determine what they are able to keep in place based on the CEC and suspend those requirements that are either ineffective or non-functioning.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Exelon suggests also adding CIP Exceptional Circumstance language in these requirements:

1. CIP-010-2, R1, Part 1.1 Develop Baseline
2. CIP-010-2, R1, Part 1.2 Authorize changes to the baseline
3. CIP-010-2, R1, Part 1.3 Update baseline

The same justification that was used for CIP-010-2, R1, Part 1.5 could be applied to these three requirments.

It is a general practice that the baseline must be created prior to the Cyber Asset being put into production. If during a declared CIP Exceptional Circumstance, a new Cyber Asset type for which an existing baseline configuration does not exist must be deployed, the development of the baseline may hinder recovery and addressing BES reliability.

Additionally, where a major system outage has occurred that qualifies as a declared CIP Exceptional Circumstance, it is possible that in the interest of restoring the reliability function a new firmware version or version of software needs to be installed on the Cyber Asset outside of the traditional rigor of the change and configuration managmenet processes.

Lastly, during a declared CIP Exceptional Circumstance it may not be practical to update the baseline within 30 days while resources are addressing the CIP Exceptional Circumstance event.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS respectfully recommends that the SDT consider the addition of the CIP Exceptional Circumstances language to the following requirements: CIP-006, R1.4 – 1.7; (may be unable to perform under CEC, i.e., if the facility is destroyed); CIP-010-2, R1.1 (may impede recovery to the detriment of restoration of a reliable BES).	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy recommends that the CIP Exceptional Circumstance language be implemented across the entire suite of CIP standards and requirements. CEC(s) are implemented in situations where safety or reliability of the BES is concerned. In these most important instances, we believe it is appropriate to address the immediate safety or reliability issue first, without concern for the compliance implications that could result. Having CEC(s) as an option for all CIP requirements would eliminate the potential for an entity to take time to rationalize, and deliberate on compliance implications, prior to mitigating a safety or reliability issue. Mitigating concerns for safety and the reliability of the BES should always be first, and an entity having the ability to claim a CEC when necessary for all CIP requirements would help reinforce this way of thinking. Duke Energy recognizes that the SDT considered a holistic approach but abandoned it since it would require CMEP changes such that it wouldn't be considered as a non-compliant event. However, Duke Energy recommends that this could be solved by simply including the phrase "except during CIP Exceptional Circumstances" at the conclusion of each individual CIP requirement.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	Yes
Document Name	

Comment

In addition to the Parts identified, we recommend adding the “except during CIP Exceptional Circumstances” language to the following Parts of the CIP Standards.

- CIP-003-7 (i) R2 Attachement 1, section 2 – In a catastrophic event, physical access controls may be affected or altered temporarily. (e.g. Katrina)
- CIP-004-6 Parts 4.2, 4.3, 4.4 – Scheduled quarter, annual, or 15 month reviews may not be delayed or not possible in the event of a catastrophic event.
- CIP-04-6, Parts 5.2, 5.3, 5.4, 5.5 – In a catastrophic event, termination and access revocation activitities may be affected.
- CIP-006-6 – 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.10, 3.1 – In a catastrophic event, physical access controls may be affected or altered temporarily (e.g., damage to gate cause by debris, or first responders entering facility).
- CIP-010 Part 1.3 – The timing of being able to update the baseline within 30 days may not be able to be completed after a catastrophic event.
- CIP-010 Part 1.4.2 – Although the timing of the testing of the cybersecurity controls isn’t addressed in the language of the requirement, there appears to be an expectation that testing occur soon after the change. In a catastrophic event, the timing of the actual testing needs to be prioritized after the recovery process is completed.
- CIP-010 Part 2.1 -- The timing of being able to update the baseline within 30 days may not be able to be completed after a catastrophic event.
- CIP-010 Parts 3.1, 3.2 – The timing of scheduled vulnerability assessments (paper or active) may be affected in the event of a catastrophic event.
- CIP-011 Part 2.2 – In a catastrophic event, the cyber asset may not be able to be found (e.g., picked up by a tornado)

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6

Answer	Yes
Document Name	

Comment

CIP-004-6, R5, Part 5.1 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. During certain events, the ability to remove access may not be possible if a system is damaged or destroyed.

CIP-006-6, R1, Part 1.2 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. In the event of a failure of a PACS, it may not be possible to have 1 factor for access control.

CIP-006-6, R1, Part 1.3 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. In the event of a failure of a PACS, it may not be possible to have 2 factors for access control.

CIP-006-6, R1, Part 1.4 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. In certain events, monitoring may not be possible if the facility is damaged or destroyed.

CIP-006-6, R1, Part 1.5 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. In the event monitoring is unavailable, alerting may not be possible.

CIP-006-6, R1, Part 1.6 Rationale - This is similar to CIP-006-6 Requirement R2, Part 2.2. In certain events, monitoring may not be possible if the facility is damaged or destroyed.

CIP-006-6, R1, Part 1.7 Rationale – This is similar to CIP-006-6 Requirement R2, Part 2.2. In the event monitoring is unavailable, alerting may not be possible.

CIP-007-6, R2 Part 2.2 Rationale - This is similar to CIP-007-6 R4, Part 4.1. Security Patch Management timeline may be unattainable if there is failure of the patch assessment system during the event.

CIP-007-6, R4 Part 4.2 Rationale - This aligns to CIP-007 R4, Part 4.1. In the event monitoring under Part 4.1 is unavailable, alerting may not be possible.

CIP-007-6, R4 Part 4.4 Rationale - This aligns to CIP-007 R4, Part 4.1. In certain events, logging may not be possible if asset or a facility is damaged or destroyed.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

CIP Exceptional Circumstances should be applied to Attachment 1, Section 3 Electronic Access Controls. Electronic access controls applied to Low BES Cyber Systems (BCS) may need temporarily bypassing due to a CIP Exceptional Circumstance. Examples are where a firewall or data diode used for Low BCS Electronic Access Controls must be temporarily bypassed to resolve the CIP Exceptional Circumstance.

Likes 0	

Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	

Seattle City Light would like to see CIP Exceptional Circumstances added to CIP-003 R2, Attachment 1, Section 2 (and Section 5, as proposed).

For Section 2, the revision would read: “***Except during CIP Exceptional Circumstances***, each Respnosbile Entity shall control physical access,…”

The rationale for this addition is similar to that for requirements associated with CIP-004 and CIP-006, in that for during certain events, access controls may not be possible if the facility is damaged or destroyed.

For Section 5, the rationale would be the same as for CIP-010 R4, extended from Transient Cyber Assets and Removable Media at High and Medium location to those at Low locations.

Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

SRP would like the following CIP requirements to be added to the CEC list of requirements:

- CIP CIP-007-6 R4, Part 4.2: If logging is unavailable due to a CEC for CIP-007-6 Part 4.1, generating alerts for security events for Part 4.1 would most likely be unavailable as well.
- CIP-007-6 R4, Part 4.4: If logging is unavailable due to a CEC for CIP-007-6 Part 4.1, reviewing logs would not be possible for the time the logging system is down during the CEC, which may exceed 15 calendar days.

Likes 0	
Dislikes 0	

Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Recommend adding the CIP Exceptional Circumstances language to the following Requirement in addition to those already identified: **CIP-006 R1, Part 1.1 – 1.9: Implementation of all Parts would be impacted by a CIP Exceptional Circumstance.**	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
CIP-006 R1 Parts 1.4 (Monitor PSP), 1.5 (Alarm within 15 minutes), 1.6 (Monitor PACS), 1.7 (Alarm within 15 minutes). Achieving compliance for these requirements depends greatly on hardware availability, including power supply. Whereas CIP-007 monitoring and logging requirements cannot be achieved in the event of a power outage to an ESP because there is no traffic flowing and without power there essentially is no ESP, the CIP-006 requires monitoring of the PSP which exists and can be accessed regardless of power outage/hardware failure/ natural disaster. Alarms cannot be generated, badge logs collected, or camera footage recorded in the event a site or system goes dark. It may be best practice for an entity to dispatch a security guard or other personnel to a site to perform manual monitoring and/or logging for some small scale events that would meet CIP Exceptional Circumstances. However, during major event such as a hurricane affecting dozens of sites across a large geographical area, it may not be feasible or within an entities safety policy to dispatch security personnel. Entities should implement compensating measures, such as fail-secure doors, for events that would affect the systems that meet compliance with these requirements during normal operations. However, it is unreasonable to expect entities to monitor and alarm at sites without appropriate support from technical solutions. Using the NERC language above, “During certain events,” physical alarming and/or monitoring “may not be possible if the facility is damaged or destroyed.”	
Likes 0	
Dislikes 0	
Response	

Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
CIP-007-6 part 2.2: If a security patch gets released 34 days after your assessment of the most recent previous patch, an entity would have one day (or possible less) to evaluate the patch. If you patch assessment system has a hardware failure (i.e. CEC) during this time, as it is now written this would be a violation. Strongly suggest adding this to the CEC list of requirements. CIP-007-6 part 4.2: If CEC is available for part 4.1 "logging of events" then it would, by inference, necessitate to have CEC available for part 4.2 since generation of alerts is probably based on logging of the events. CIP-007-6 part 4.4: Additionally for the same reason part 4.4 reviewing a summarization or sampling of logs would not be possible if all logging was offline during the CEC event, and the CEC event lasted more that 15 calendar days.	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

9. If you have additional comments on the proposed approach that you have not provided in response to the questions above, please provide them here.

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4

Answer	
Document Name	

Comment

When possible, consider adding the CIP Exceptional Circumstances language at the Requirement level rather than each of the individual Parts.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	
Document Name	

Comment

n/a

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	
Document Name	

Comment

Seattle asks that the Standards Drafting Team consider simplifying the application of CIP Exceptional Circumstances to parts of CIP-006 by applying CIP Exceptional Circumstance language to R1 and R2, rather than to various parts and sub-parts.

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	

A Reliability Standard must not hinder REs in responding to situations that endanger human life and/or adversely impact system restoration.

It is possible to devise a circumstance where every one of the NERC CIP Reliability Standards may be violated while responding to a CIP Exceptional Circumstance. Instead of the proposed piecemeal approach, it is more reasonable to add a single requirement giving REs flexibility to respond to CIP Exceptional Circumstances that covers all NERC CIP requirements. NERC CIP-003 is a logical location for such a requirement.

Embedding one universally applicable CIP Exceptional Circumstances requirement provides an approach that resolves the immediate dilemma of requirements for which an RE cannot possibly comply. During the normal course of standards revisions, legacy individual CIP Exceptional Circumstance clauses could be organically phased out so as not to induce a flurry of undue burden in otherwise unsubstantive procedure revisions.

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6	
Answer	
Document Name	
Comment	

Documentation requirements associated with “documenting” the results of a previous Part, such as CIP-010 Part 3.4, should not require CEC language provided the language is afforded to the Parts subject to CEC treatment. In this example, CIP-010 Parts 3.1, 3.2, 3.3. However, if CEC is not extended to all of the Parts (CIP-010 Parts 3.1, 3.2, 3.3), then it should be considered for the documentation requirement (in Part 3.4).

Likes 0	
Dislikes 0	
Response	

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	
Document Name	
Comment	
Not at this time.	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	
Document Name	2016-02_CIP_CEC_Unofficial_Comment_AZPS.docx
Comment	
AZPS would like clarification on the following statement: “CEC are included in a Responsible Entity’s cyber security policy from CIP-003 which describes how the entity would declare and respond to a CEC. During a declared CEC, the entity is allowed exception(s) to adhering to the specific reliability objective of the requirement(s); however, the entity is still compliant with the requirement(s) if the entity properly declares and responds to the CEC and adheres to its applicable cyber security policies”. The last phrase appears to contradict the concept or philosophy being expressed in the previous phrase in that it appears to require the entity to remain compliant with the requirement even if such requirement is impacted by a CEC. This would be contrary to the intent of a CIP Exceptional Circumstance	

wherein it is recognized that a responsible entity's ability to be compliant may be impacted as a result of a CEC, e.g., if a facility is substantially destroyed, a physical security perimeter may no longer be intact. AZPS requests that the SDT clarify the statement to ensure that the effect of declaring a CEC is clear and that all responsible entities understand what their continuing obligations are once a CEC is declared. Addtionally, AZPS has attached a document with recommendations to the Rationale in the table titled List of Additional Requirements for Consideration on Page 2-4 of the Unofficial Comment Form.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
Consider simplifying the application of CEC in CIP-006 by applying the term to R1 and R2 and not to the sub-sections.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's comments in response to #1.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	

Answer	
Document Name	
Comment	
AEP recognizes the considerable effort of the SDT to establish an expansion of CIP requirements subject to exception during a CEC. AEP is concerned that like Versions 5 and 6 it will later be found that additional requirements should be subject to exception during a CEC. A more general rule for exceptions to CIP requirements would allow entities additional flexibility to manage its response during a CEC and future proof the CIP Standards in this area. The flexibility should come with a requirement to justify anyexceptions to requirements taken at specific locations or regions as they are impacted by a CEC. This or similar language could be placed in the "Exceptions" section of each CIP Reliability Standard: "4.2.3.5. A Responsible Entity may temporarily suspend compliance activities associated with CIP requirements for affected assets, BES Cyber Systems and individuals during a period when it has declared a CIP Exceptional Circumstance". And, language could be added to the existing policy requirements of CIP-003-7 as follows: R1 1.1.9. and 1.2.6 **"**Declaring, justifying and responding to CIP Exceptional Circumstances".	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
ERCOT supports the drafting team's position in adding the CEC language to additional requirement parts. Although a formal CEC program would have been beneficial to entities in allowing coverage for all requirements, introducing compliance that derived from the approach would be burdensome to have all instances of invoking a CEC result in potential non-compliance.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - SPP RE,RF	
Answer	
Document Name	
Comment	

CIP Exceptional Circumstances include both a Bulk Electric System emergency when the responsible entity is delayed in, or prevented from, performing or carrying out any compliance activity required by CIP-002 through CIP-014 by reason of or through any cause reasonably beyond its control and not attributable to its neglect .

During the threat and after the impact of a CIP Exceptional Circumstance, ITC's priorities are the safety of its' employees and customers, environment compliance and the restoration of service.

Likes 0	
Dislikes 0	

Response

Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF

Answer	
Document Name	

Comment

Consider whether any changes to the definition of CIP Exceptional Circumstances are needed to accommodate potential government (Executive, DOE, etc.) orders which may require us to behave in a manner that appears to be out of compliance with one or more requirement(s) which provides for CIP Exceptional Circumstances.

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	
Document Name	

Comment

Basin Electric Power Cooperative agrees with the discussion surrounding the identification of typical standards/requirement/parts likely to be affected by a CIP Exceptional Circumstance. However, Basin Electric would prefer the removal of CIP Exceptional Circumstance Language on a per standard/requirement/part level and instead focus on CIP-003 enhancements and related Implementation Guidance. The overhead of including the exception in multiple standards/requirements/parts seems to outweigh the benefit of a low frequency circumstance.

Likes 0	

Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
Reclamation recommends clarification on what evidence will be required for a CIP Exceptional Circumstance.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	
Document Name	
Comment	
Consider simplifying the application of CEC in CIP-006 by applying the term to R1 and R2 and not to the sub-sections.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	

Compliance with many additional CIP requirements could be impacted by a CIP Exceptional Event. Any requirement with an established timeframe (24 hours, 30 days, 15 months, or 7 years) could be impacted if a compliance requirement is slated for completion near the end of the time period and a CIP Exceptional Event were to occur.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	
Document Name	

Comment

Tacoma supports the comments of Utility Services, Inc

Likes 0	
Dislikes 0	

Response

Additional comments received by Vivian Vo of APS (Q9)

List of Additional Requirements for Consideration

Standard	Requirement	Rationale
CIP-004	Requirement R3, Part 3.5 Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	This is similar to the CIP-004-5 Requirement R2, Part 2.2 training requirement. A personnel risk assessment cannot be performed on first responders, would not be possible in emergency circumstances, and may not be possible on relevant vendors. Thus, this requirement should be subject to CIP Exceptional Circumstances for both ~~is would cover~~ the entity's personnel as well as contractors and service vendors
CIP-006	Requirement R1, Part 1.8 Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	This aligns to CIP-006-6 Requirement R2, Part 2.2. During certain events, logging may not be possible if the facility in which the logging and/or supporting hardware, software, or communication networks reside is damaged or destroyed. Thus, this requirement should be subject to CIP Exceptional Circumstances.
CIP-006	Requirement R1, Part 1.9 Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	This aligns to CIP-007-6 Requirement R4, Part 4.3. During certain events, a facility where the logging and/or supporting software, hardware, or communications reside may be damaged or destroyed. As a result, records already recorded for retention may also be adversely impacted and new logging may not be possible~~ if the facility is damaged or destroyed~~. Thus, this requirement should be subject to CIP Exceptional Circumstances.
CIP-006	Requirement R2, Part 2.3 Retain visitor logs for at least ninety calendar days.	This aligns to CIP-007-6 Requirement R4, Part 4.3. During certain events, a facility where the logging and/or supporting software, hardware, or communications reside may be damaged or destroyed. As a result, records already recorded for retention may also be adversely

Standard	Requirement	Rationale
		impacted and new logging may not be possible. Thus, this requirement should be subject to CIP Exceptional Circumstances.~~During certain events, logging may not be possible if the facility is damaged or destroyed.~~
CIP-007	Requirement R4, Part 4.1 Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	This aligns to CIP-006-6 Requirement R2, Part 2.2. During certain events, if the facility in which hardware, software, or communication networks utilized to support logging of events resides is damaged or destroyed, the ability to log events could be adversely impacted. Thus, this requirement should be subject to CIP Exceptional Circumstances.~~During certain events, logging may not be possible if the facility is damaged or destroyed.~~
CIP-010	Requirement R1, Part 1.4.1 Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;	This aligns to Requirement R3, Part 3.3. During ~~the~~ an event, security controls identification and testing may impede recovery efforts necessary to restore the reliable operation of the BES. Thus, this requirement should be subject to CIP Exceptional Circumstances.
CIP-010	Requirement R1, Part 1.5 Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and	This aligns to Requirement R3, Part 3.3. During an event, security controls identification and testing may impede recovery efforts necessary to restore the reliable operation of the BES. Thus, this requirement should be subject to CIP Exceptional Circumstances.~~During the event, security controls testing may impede recovery efforts.~~

Standard	Requirement	Rationale
	CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	

Additional comments received from Nathan Mitchell of APPA

Questions

Note: The new (revised) language is shown in red text.

1. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-004 R3, Part 3.5: Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years, except during CIP Exceptional Circumstances.

   ☒ Yes

   ☐ No

   Comments:

2. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-006 R1, Part 1.8: Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.

   ☒ Yes

   ☐ No

   Comments:

3. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-006 R1, Part 1.9: Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.

☒ Yes

☐ No

Comments:

4. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-006 R2, Part 2.3: Retain visitor logs for at least ninety calendar days, except during CIP Exceptional Circumstances.

   ☒ Yes

   ☐ No

   Comments:

5. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-007 R4, Part 4.1: Log events, except during CIP Exceptional Circumstances, at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

   ☒ Yes

   ☐ No

   Comments:

6. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

   CIP-010 R1, Part 1.4.1: Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change.

   ☒ Yes

   ☐ No

   Comments:

7. Do you agree with adding the existing CIP Exceptional Circumstance language to the Requirement/Part listed below? Please provide a detailed explanation/rationale for inclusion or exclusion of the CEC language.

CIP-010 R1, Part 1.5: Where technically feasible, for each change that deviates from the existing baseline configuration:

1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected, except during CIP Exceptional Circumstances; and

1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments, except during CIP Exceptional Circumstances.

☒ Yes

☐ No

Comments:

8. Are there other Requirement(s) or Part(s) that should include the CIP Exceptional Circumstance language other than those already identified in this request? If so, please identify and provide the rationale.

☒ Yes

☐ No

Comments:

Include the electronic and physical security controls required by CIP-003 R2 Attachment 1, sections 2 and 3. This would meet the same rational as used for the inclusion of CEC for CIP-004 and CIP-006.

9. If you have additional comments on the proposed approach that you have not provided in response to the questions above, please provide them here.

Comments:

Consider simplifying the application of CEC in CIP-006 by applying the term to R1 and R2 and not to the sub-sections.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Virtualization in the CIP Environment

Do not use this form for submitting comments. Use the electronic form to submit comments on the **use of Virtualization in the CIP environment**. The electronic form must be submitted by **8 p.m. Eastern, Tuesday, April 11, 2017**.

Additional information is available on the project page. If you have questions, contact Mat Bunch (via email) or at (404) 446-9785.

Background Information

On January 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards,* approving seven CIP Reliability Standards and new or modified definitions. On March 9, 2016, the NERC Standards Committee authorized a Standards Authorization Request (SAR) to be posted for a 30-day informal comment period from March 23 – April 21, 2016. Based on the comments received, the Standard Drafting Team (SDT) made minor revisions to the SAR which was posted for an additional 30-day informal comment period June 1-30, 2016.

The purpose of this project is to; (1) consider the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for Standard Drafting Team Consideration (V5TAG Transfer Document), and (2) address the Commission directives contained in Order 822. These revisions will increase reliability and security to the Bulk Power System (BPS) by enhancing cyber protection of BPS facilities.

The V5TAG, which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by the existing SDT for the CIP Reliability Standards. The V5TAG developed the V5TAG Transfer Document to formally recommend that the SDT address these issues during the standards development process and to consider whether modifications can be made to the standard language.

The current informal posting document is an effort to gather input on the V5TAG issue related to virtualization in the CIP environment. The CIP standards are based primarily on concepts dating back to Version 1 and as technology has evolved, issues have begun to arise as entities attempt to take new concepts and fit them into some of the Version 1 paradigms. These issues revolve around topics such as:

- Hypervisor – the virtualization component that manages the guest operating systems (OSs) on a host and controls the flow instructions between the guest OSs and the physical hardware.

- Virtual machines – With virtualization technologies, a single physical Cyber Asset can be used as an execution platform for numerous virtualized operating systems, micro-service containerized applications, and virtual network functions of all classifications. A single physical Cyber Asset can appear to an external network as many complete Cyber Assets. Virtual switches and networks can be defined so these virtual machines can communicate with each other as if they are separate physical nodes on the network. Virtual machines and functions can also migrate around a physically clustered cyber system such that the singular physical Cyber Asset where an application resides can change at any moment.

  The virtualization of Cyber Assets provides advantages for the availability, resiliency, and reliability of applications and functions hosted in such an environment and the CIP standards must not stand in the way of these benefits as long as they are implemented in a secure manner. Virtualization affords enhanced security in some cases as the security controls themselves can be virtualized and placed within the virtual environment closer to the workloads they are protecting. However, there are also different security risks introduced by these environments. The management systems or consoles for these environments allow for the complete control of numerous components of the infrastructure. Virtual machines or networks can be added, modified, or deleted from one central management system. For example, rogue virtual components can starve legitimate workloads of the shared resources (processor, memory, etc.) they need to reliably perform their function. In summary, changes to the CIP Requirements may be needed to account for virtualization.

- Virtual Networks – Electronic Security Perimeter (ESP) constructs within the current CIP standard are limited to defining security zones at Open Systems Interconnection (OSI) Layer 3 and do not support security zones defined at layers other than OSI Layer 3. With current, widely deployed technology, networks are no longer solely defined by the arrangement of physical hardware and cables *inside* or *outside* of a *perimeter*. Networks can exist as a mixture of physical and virtual segments or purely in a virtual state within one device. Virtual firewalls and other security tools are also available to help secure these environments. Typical hardware network switches can be configured with internal logical isolation to implement multiple virtual networks within them. Accordingly, the SDT is reviewing the CIP standards to validate that definitions, requirements, and guidance regarding ESPs and Electronic Access Points (EAPs) continue to provide for secure and reliable operations.

- Virtual Storage – Historically, servers were limited to dedicated storage within the device. Typically, the operating system and the applications resided in the server on hard drives. Virtual storage technologies such as Storage Area Networks (SANs) present virtualized logical drive storage units to all attached servers. These types of environments then become a shared resource among many physical and virtual hosts.

With all of this in mind, the SDT is considering:

1) Areas in the current CIP requirements that might prevent or hinder the adoption of virtualization technologies for BES Cyber Systems and related systems;

2) Areas of new risks introduced by virtualization technologies and how to address them in the standards.

Questions

The SDT has determined that some of the concepts in CIP Version 5 must be fully realized in order to support virtualization. For example, while Version 5 introduced the “cyber system” concept and most requirements are now written at the cyber system level, the advantages of this approach have not been fully integrated into all levels of planning, design or compliance assessment approaches. Most entities still manage their CIP programs at a device level and auditors still look for device-centric evidence of compliance. This paradigm poses substantial issues with the use of virtual technologies. Infrastructure resources are pooled, apportioned to a given workload, and withdrawn or re-assigned when no longer needed. Infrastructure components (including instances of operating systems) come and go according to the current workload, making individual Cyber Asset level inventories difficult or impossible. The mobility of these resources makes permanently describing their physical locations problematic. Hardware (both computer and network) becomes a general-purpose commodity — merely a pool of resources on top of which the actual infrastructure is designed and created at a logical/virtual level. As technology increasingly blurs the line between physical and virtual systems, managing compliance in terms of individual devices or Cyber Assets becomes more challenging.

1. Version 5 introduced the BES Cyber System concept, and requirements reference applicability at the *BES Cyber System* level. However, language in the measures shows that, implicitly, many controls are expected to be implemented at the *BES Cyber Asset* or *device* level. The SDT assumes that most auditors expect entities to demonstrate compliance at the device level. Do you agree with the SDT’s assumption? If so, how should the SDT address these inconsistencies?

   ☐ Yes
   ☐ No

   Comments:

To incorporate virtualization and address the V5TAG transfer issue to clarify the meaning of the term *programmable* in the current definition of *Cyber Assets*, the SDT is proposing changes to the definition that include defining the term in the singular rather than the plural. Updating the definition to include virtual environments allows the definition of other terms based on *Cyber Asset*, such as Electronic Access Control or Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) to also include virtual environments.

The proposed *Cyber Asset* definition is:

> Redlined
> *~~Programmable~~An electronic device~~s~~ (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in ~~those devices~~ the device. A virtual machine is itself a distinct asset from its host(s).*
>
> Clean
> *An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).*

2. The SDT proposes that each virtual machine and hypervisor are separate Cyber Assets. Do you agree with this position? Please provide a rationale to support your position.

   ☐ Yes
   ☐ No

   Comments:

3. Do you agree that the proposed Cyber Asset definition clarifies the term *programmable*? Please provide a rationale to support your position.

   ☐ Yes
   ☐ No

   Comments:

In virtualized environments, the physical infrastructure can be shared between BES Cyber Systems and other non-CIP Cyber Assets while maintaining isolated virtualized environments for each.

4. Such configurations are not addressed explicitly in CIP-005-5. Are modifications required to address the issue? Please provide your rationale.

   ☐ Yes
   ☐ No

   Comments:

Concerning virtual networks, network devices can have multiple logical networks configured (e.g. virtual local area networks (VLANs)). Physical or virtual devices perform “logical isolation” when configured such that some network interfaces are available inside an ESP, and other interfaces are outside an ESP and the two networks cannot communicate with each other inside of the device. This would not prevent the VLANs configured inside the device from communicating through an EAP.

5. The SDT asserts that VLANs providing logical isolation are not addressed explicitly in CIP-005-5, and controls may be necessary to isolate BES Cyber Systems. Are the current requirements of CIP-005-5 sufficient to address logical isolation using VLANs? Please provide your rationale.

   ☐ Yes
   ☐ No

   Comments:

The SDT has identified certain risks inherent to virtualization regarding the use of centralized management automation. The SDT is proposing to classify *Centralized Management System* (CMS) explicitly as a type of applicable system for some CIP requirements. In examining management architecture and risk management for virtual environments, the SDT identified an increased risk inherent to the span of control of hypervisor management consoles. Further, the SDT noted that similar risks exist in CMSs used to manage physical devices, and recognized these risks may not be fully addressed in current CIP standards and the *EACMS* definition. The SDT is considering a new definition of this class of system.

The proposed *Centralized Management System* (CMS) definition is:

> *A centralized system for administration or configuration of BES Cyber Systems, including but not limited to systems management, network management, storage management, or patch management.*

6. Do you agree with the proposed definition of CMS? If not, please provide alternative language for the definition and your rationale.

   ☐ Yes
   ☐ No

   Comments:

7. Do you agree with the SDT's approach to reference the CMS specifically as a type of applicable system in the CIP standards? Please provide your rationale.

   ☐ Yes
   ☐ No

   Comments:

In examining virtualization, the SDT considered centralized management systems or consoles for these environments. These systems allow for the mass addition, deletion and modification of virtual machines and networks. Access to the control surface of a cyber system is known as the *management plane*. The management plane is where the virtual infrastructure is configured and managed by a limited group of administrators as opposed to the *data plane*. The data plane is where the end user's access to the virtual machine's business function takes place. To meet the security objective of protecting a BES Cyber System from threats in the data plane, the management plane should be isolated from the data plane. These types of controls are referred to as *out of band* management.

The SDT is considering limiting the scope of management plane protection requirements to high and medium impact Control Centers because these environments contain the highest risk.

8. Do you agree with the SDT's approach to require the isolation between the data plane and the management plane? Please provide your rationale.

   ☐ Yes
   ☐ No

   Comments:

9. Do you agree with limiting the applicability to high and medium impact Control Centers? Please provide your rationale.

   ☐ Yes
   ☐ No

   Comments:

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Announcement

2016-02 Modifications to CIP Standards
Transmission Owner Control Center Performing Transmission Operator Obligations and Virtualization

Informal Comment Periods Open through April 11, 2017

Now Available

The Project 2016-02 Standard Drafting Team (SDT) is requesting stakeholder input on two issues it is addressing from the Version 5 Transition Advisory Group (V5TAG): (1) the applicability of the CIP Reliability Standards to BES Cyber Systems for a Transmission Owner Control Center performing the functional obligations of a Transmission Operator; and, (2) the use of virtualization in the CIP environment. Two concurrent 29-day informal comment periods are open through **8 p.m. Eastern, Tuesday, April 11, 2017,** for stakeholders to provide feedback on the SDT's approach and draft language for each issue.

Commenting

Use the electronic form to submit comments. If you experience any difficulties using the electronic form, contact Wendy Muller. Unofficial Word versions of the comment forms are posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The drafting team will review all responses received and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance regarding TOCC, contact Senior Standards Developer, Al McMeekin (via email) or at (404) 446-9675. For additional assistance regarding Virtualization, contact Standards Developer, Mat Bunch (via email) or at (404) 446-9785.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization
Comment Period Start Date:	3/14/2017
Comment Period End Date:	4/11/2017
Associated Ballots:	

There were 54 sets of responses, including comments from approximately 136 different people from approximately 89 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Version 5 introduced the BES Cyber System concept, and requirements reference applicability at the *BES Cyber System* level. However, language in the measures shows that, implicitly, many controls are expected to be implemented at the *BES Cyber Asset* or *device* level. The SDT assumes that most auditors expect entities to demonstrate compliance at the device level. Do you agree with the SDT's assumption? If so, how should the SDT address these inconsistencies?

(Refer to the Unofficial Comment Form for more information on this question)

2. The SDT proposes that each virtual machine and hypervisor are separate Cyber Assets. Do you agree with this position? Please provide a rationale to support your position.

(Refer to the Unofficial Comment Form for more information on this question)

3. Do you agree that the proposed Cyber Asset definition clarifies the term *programmable*? Please provide a rationale to support your position.

(Refer to the Unofficial Comment Form for more information on this question)

4. In virtualized environments, the physical infrastructure can be shared between BES Cyber Systems and other non-CIP Cyber Assets while maintaining isolated virtualized environments for each.

Such configurations are not addressed explicitly in CIP-005-5. Are modifications required to address the issue? Please provide your rationale.

5. The SDT asserts that VLANs providing logical isolation are not addressed explicitly in CIP-005-5, and controls may be necessary to isolate BES Cyber Systems. Are the current requirements of CIP-005-5 sufficient to address logical isolation using VLANs? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

6. Do you agree with the proposed definition of CMS? If not, please provide alternative language for the definition and your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

7. Do you agree with the SDT's approach to reference the CMS specifically as a type of applicable system in the CIP standards? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

8. Do you agree with the SDT's approach to require the isolation between the data plane and the management plane? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

9. Do you agree with limiting the applicability to high and medium impact Control Centers? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	1,3,4		FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Midcontinent ISO, Inc.	David Francis	2	MRO,NPCC,RF,SERC,SPP RE,Texas RE,WECC	SRC + SWG	Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Terry BIlke	Midcontinent ISO, Inc.	2	RF

					Elizabeth Axson	Electric Reliability Council of Texas, Inc.	2,3	Texas RE
					Ben Li	IESO	1	MRO
					Drew Bonser	SWG		NA - Not Applicable
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
BC Hydro and Power Authority	Patricia Robertson	1,3,5		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC
					Venkataramakrishnan Vinnakota	BC Hydro and Power Authority	2	WECC
					Pat G. Harrington	BC Hydro and Power Authority	3	WECC

					Clement Ma	BC Hydro and Power Authority	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion and ISO-NE	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC

					Quintin Lee	Eversource Energy	1	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Steven Keller	Southwest Power Pool Inc.	2	SPP RE
					John Allen	City Utilities of Springfield, Missouri	4	SPP RE
PSEG	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF
AEP	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Prairie Power, Inc.	PPI	1,3	SERC
					Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF
					Sunflower Electric Power Corporation	SEPC	1	SPP RE
					Great River Energy	GRE	1,3,5,6	MRO
					North Carolina Electric Membership Corporation	NCEMC	3,4,5	SERC

					Rayburn Country Electric Cooperative	RCEC	3	SPP RE
					Buckeye Power, Inc.	BUCK	4	RF
					Southern Maryland Electric Cooperative	SMECO	3	RF
					Wabash Valley Power Association	WVPA	3	SERC

1. Version 5 introduced the BES Cyber System concept, and requirements reference applicability at the *BES Cyber System* level. However, language in the measures shows that, implicitly, many controls are expected to be implemented at the *BES Cyber Asset* or *device* level. The SDT assumes that most auditors expect entities to demonstrate compliance at the device level. Do you agree with the SDT's assumption? If so, how should the SDT address these inconsistencies?

(Refer to the Unofficial Comment Form for more information on this question)

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not agree with the SDT's assumption about the expectation of auditors and believes each entity should have the flexibility to defend compliance decisions based on the requirement language in the CIP Standards. Entities may find some controls easier or more effective to implement and provide evidence at a BES Cyber System level rather than at the BES Cyber Asset or device level, or vice versa depending on the requirement and the current CIP Standards provide this option.

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	No
Document Name	

Comment

For some of the standards, like anti-virus/malware protection, a holistic approach can yield a design that protects assets without being draconian regarding the installation of anti-virus/malware protective software on every individual asset. Peak suggest the SDT consider real-world scenarios for situations and decide, for each standard, which ones can be addressed on an individual-asset basis only, and which ones can be addressed at the BES Cyber System level.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	No

Document Name	

Comment

Entergy understands that entities must be able to prove that each device that is part of a BES Cyber System need to be evaluated for compliance, but expect the distinction to be that controls do not have to be implemented at the individual device level provided evidence can prove the they benefit from controls implemented at the BES Cyber System level. For example, depending on the architecture every device may benefit from Intrusion Prevention Systems (IPS) with deep packet inspection for malware prevention, but that does not mean IPS is running on each individual device.

To incorporate virtualization and address the V5TAG transfer issue to clarify the meaning of the term *programmable* in the current definition of *Cyber Assets*, the SDT is proposing changes to the definition that include defining the term in the singular rather than the plural. Updating the definition to include virtual environments allows the definition of other terms based on *Cyber Asset*, such as Electronic Access Control or Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) to also include virtual environments.

The proposed *Cyber Asset* definition is:

An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	

Comment

The SDT should consider removing or further clarifying the purpose of including language (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) [see CIP-007-6, Part 4.1]. Additionally, the SDT could consider adding in the Appplicable Systems language, ‘and their associated BES Cyber Systems:’ if the intent of CIP v5 was to leverage a system-centric approach to affording the required controls for all Cyber Assets.

This may require the same change in the purpose statement found in all CIP Reliability Standards:

‘To identify and categorize BES Cyber Systems and their associated BES Cyber Assets…’

The SDT may want to reconsider the following cyber system concept paper –

http://www.nerc.com/docs/standards/sar/Concept_Paper_Categorizing_Cyber_Systems_2009July21.pdf

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

It has been BPA’s experience that guidance provided to auditors leads them to expect and look for controls to be applied to the Cyber Asset. Also, they seem skeptical of implementations where a given device performs a portion of the control function and additional components of the security strategy are implemented across multiple devices on the network. Auditors might consider only the device portion of an overall control and evaluate it outside of the network-based defense-in-depth strategy.

One way to address this inconsistency would be to normalize the use of the term “system” across the example measures rather than “device” wherever applicable. The SDT should add Guidance in the Technical Basis sections to clarify that defense in depth strategies are desirable. The Electronic Access Control and Monitoring System (EACMS) paradigm should be revised in line with standard IT Security practice and terminology as performing Authentication, Authorization, and Accounting (AAA). It is also important to explicitly allow for distributed systems to perform this AAA function for a security zone rather than the legacy concept of hardened perimeter.

There may also be a need to revisit the Reliability Standards Audit Worksheets in light of system vs device to provide better guidance to auditors attempting to apply the questions in the RSAW to an entity’s evidence.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	Yes
Document Name	

Comment

Dominion agrees with the statement that it appears auditors are expecting entities to show compliance at the device level for CIP v5 standards. However, the standard clearly allows compliance to be demonstrated at the system level. If the applicability of the controls is at the system level, then controls can be at the system level OR at the device level (where each device in the system has appropriate controls). If the applicability of the standards is intended to be at the BCA level, the applicability column clearly state that the expectation is for monitoring to occur at that level. To reinforce the applicability at the system level, the SDT should include specific system examples in the Measures section and similar system examples in the GTB or an Implementation Guidance document.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Exelon agrees with the assumption that the current expectation from auditors is to see compliance demonstrated at the BCA or device level. We view this as a concern that should be addressed, and we would welcome more clarity in the guidance on when device level compliance is required versus when protections can be demonstrated at the BES Cyber System level.

In the meantime, Exelon does continue to demonstrate compliance down to the BCA and device level, including all individual logical or virtual machines as well as their VM Host machine(s).

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF

Answer	Yes
Document Name	

Comment

It was PJM’s experience during our version 5 audit that auditors did expect many controls were implemented at the device level. We found this was expected more for requirements that contained prescriptive language. Objective based controls lend themselves more to implementing controls at the BES Cyber System level. In order to help clarify how to handle the requirements for systems vs individual assets, additional guidance with respect to virtualization for both scenarios may be helpful.

Likes 0	
Dislikes 0	

Response

Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

I concur with the suggested edits. As long as this new definition is updated and incorporated throughout the CIP standards, we believe this would address any inconsistencies as to device level auditing.

Likes 0	

Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees there are inconsistencies between the language of the requirement and the measures regarding applicability of the requirements at the BES Cyber System level. It has been our experience that in some instances auditors looked at the device level instead of evaluating the controls applied at the system level. SRP utilizes a Defense in Depth security architecture, which applies controls and additional security measures across multiple devices on the network. SRP suggests the SDT add discussion of this strategy in the guidelines and technical basis section.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Yes – SMUD Agrees. Virtualization is a proven secure method for sharing physical resources, and should be incorporated as an acceptable technology for network, firewall, compute (virtual machines), and storage. The acceptance for each of the areas should be outlined such that auditors and utility companies fully understand the acceptable configurations. At a minimum, the “device level” term should be changed to “operating system” as it is inclusive for processes, data, authentication, configuration, and traffic forwarding. This “operating system” could serve as the basis for all fully virtualized functions including virtual machines, virtual routers, virtual firewalls, etc. For systems that provide services with a shared “operating system”, such as a router with multiple isolated routing tables (VRF), guidelines should summarize the constraints.	

Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST believes that most Responsible Entities have reconciled to the notion that CIP requirements should be applied on a per- Cyber Asset basis, notwithstanding the fact many requirements are formally applicable to BES Cyber Systems that may comprise multiple Cyber Assets. N&ST also believes the SDT is correct in its belief that most, if not all, auditors expect to see evidence of device-level compliance. If the SDT is convinced this should be codified by revising the Standards, N&ST suggests adding language that clarifies requirements applicable to BES Cyber Systems must be applied to each Cyber Asset comprising a given BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
To incorporate virtualization and address the V5TAG transfer issue to clarify the meaning of the term *programmable* in the current definition of *Cyber Assets*, the SDT is proposing changes to the definition that include defining the term in the singular rather than the plural. Updating the definition to include virtual environments allows the definition of other terms based on *Cyber Asset*, such as Electronic Access Control or Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) to also include virtual environments. The proposed *Cyber Asset* definition is: Redlined *ProgrammableAn electronic devices (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in those devices the device. A virtual machine is itself a distinct asset from its host(s).* Clean *An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).*	
Likes 0	

Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

CIP v5 was conceived and described to industry as a "systems-based" approach, and this conceptual framework should be promoted as much as possible. As such, Seattle City Light believes that new or revised requirements should be structured and written at the BES Cyber System level as much as possible, and new measures and VSL should be developed to reinforce the system-based approach. In some cases there may need to be new parallel VSLs for both systems and devices, but in the long run, the device-focused approach should be phased out over time.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	Yes
Document Name	

Comment

Where virtual machines behave like physical machines (run an OS such as Windows), it makes sense to request the same sort of evidence as for a physical machine that is also one component of a BES Cyber System. With regard to hypervisors due consideration should be given to their specialized nature to avoid treating them like just another OS, although change control and cybersecurity still apply.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

Add the clear definitions for Hyper Visor (as a required asset) and Virtual Server (as a required asset) and then don't be concerned with the commodity abilities to add/remove processor, memory, disk, etc. Require that Virtual Servers remain constant in an environment regardless of what physical hypervisor asset they are running at any given time. This will ensure consistency and allow for clear asset level tracking. Scaling is a normal part of operating in a virtual environment and needs to account for virtual scaling. With respect to horizontal scaling, an entity would need to have at least one consistent virtual asset that is listed on the BES Asset List with a stated program for how and when horizontal instance is created/destroyed to account for spikes in demand. The entity would need to clearly show how they protect (via a program) for CIP007 requirements as instances are created. The burden would be on each entity to prove their model of protection (which is the model other security compliance standards such as PCI take).

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF

Answer	Yes
Document Name	

Comment

ITC understands that today security is assigned at the device level and technologies have surpassed the language used in the CIP standards. Regardless, ITC recommends revising the CIP-005, CIP-007, and CIP-010 standards that reflect BES Cyber Systems to address virtualization.

We agree that controls should be applied at the device level, however, there should be specific language instead of vague and ambiguous language regarding virtualization. For instance, if a hypervisor is installed on a physical server device it should be stated that the guest OS's are all part of the same cyber asset classification. To add further clarity, if the hypervisor and physical server host BCAs then all devices should be BCAs.

The standard should offer exceptions for other methods of virtual and physical separation such as virtual firewalls, virtual switch instances, and other technologies that offer security between virtualized networks or hosts. Vendors such as CheckPoint offer VSec (a technology used to spin up virtual firewalls) both at hypervisor and host levels. Other vendors such as Cisco offer ACI technology on their Nexus 9000 switching platforms. These allow for a single layer 2 network to have enterprise security groups which isolate devices and hosts from each other.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	Yes
Document Name	

Comment

AEP has observed that Regional Entity compliance staff expect evidence at the Cyber Asset level even where the applicability to the standard is at the "Cyber System" level. Regarding the definition of Cyber Asset, AEP believes the best approach is to modify the definition of Cyber Asset to make it general enough to encompass virtual machines or virtual Cyber Assets. Additional recommendation would be to evaulate inconsistencies of Applicable Systems and Measures columns.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	Yes
Document Name	

Comment

This is an ongoing problem that extends beyond virtualization. The SDT should consider using the Applicable Systems column to address distinctions between BES Cyber System application of requirements and BES Cyber Asset application on an explicit and per requirement basis.

Is there a recommendation include in the auditors audit guide about the ways the control should be implemented? (at the *BES Cyber Asset* or *device* level) If it's the case this guide needs to be updated.

To incorporate virtualization and address the V5TAG transfer issue to clarify the meaning of the term *programmable* in the current definition of *Cyber Assets*, the SDT is proposing changes to the definition that include defining the term in the singular rather than the plural. Updating the definition to include virtual environments allows the definition of other terms based on *Cyber Asset*, such as Electronic Access Control or Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) to also include virtual environments.

An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).

Likes 0	
Dislikes 0	

Response

Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6

Answer	Yes
Document Name	

Comment

We agree that auditors look for asset level evidence for certain requirements and that the application of this expectation is consistent with the way the Standards are written. For instance, one asset may provide AV protection for an entire system; auditors will check that asset for compliance.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

Ideally, the host should be treated as the high watermark of any of the devices (should be able to operate in a mixed mode, as long as demonstratable that none of the other devices have the potential to impact a higher risk impact virtual machine). NRG recommends that the language should be rewritten to accommodate the different nuances that virtual technology presents. Especially concerning the differences between a physical desktop (device level), a standalone virtual desktop (device level), and virtual linked-clone pools (system level) which contain a virtual base/parent image and their linked clones (cloned children images). The requirement is written such that the auditors are bound to look at the system level, but all of the standards have to be applied at the device level. Ultimately the choice should be up to the entity to define how they want to set up their Virtual Environment as long as all of the security controls are in place.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE

Answer	Yes
Document Name	

Comment

This is an ongoing problem that extends beyond virtualization. The SDT should consider using the Applicable Systems column to address distinctions between BES Cyber System application of requirements and BES Cyber Asset application on an explicit and per requirement basis.

Is there a recommendation include in the auditors audit guide about the ways the control should be implemented? (at the *BES Cyber Asset* or *device* level) If it's the case this guide needs to be updated.

To incorporate virtualization and address the V5TAG transfer issue to clarify the meaning of the term *programmable* in the current definition of *Cyber Assets*, the SDT is proposing changes to the definition that include defining the term in the singular rather than the plural. Updating the definition to include virtual environments allows the definition of other terms based on *Cyber Asset*, such as Electronic Access Control or Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) to also include virtual environments.

The proposed *Cyber Asset* definition is:

Redlined

ProgrammableAn electronic devices (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in those devices the device. A virtual machine is itself a distinct asset from its host(s).

Clean

An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).

Likes 0	
Dislikes 0	

Response

Lee Maurer - Oncor Electric Delivery - 1

Answer	Yes
Document Name	

Comment

We agree with the assumption. This may be the expectation of an auditor. However, more education and guidance may be required for auditors to fully understand the technology being used by industry and how to appropriately audit it.

The requirements do allow protections to be performed at a BCS level. There are some requirements where it is easier to apply a control at a BCS level. This would include malware protection at the BCS level, patch assessment at the BCS level, and event logging at a BCS level. Conversely, there are some requirements where it is easier to demonstrate compliance at the Cyber Asset level. For us, that includes baseline of assets.

When addressing compliance with virtual systems, it will be important to have the controls allowed at the host or template level as long as the entity is capable of showing how the control is inherited by a guest.

Likes 0	
Dislikes 0	

Response

Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC

Answer	Yes
Document Name	

Comment

The BES Cyber System needs to be more defined. Utilities can declare BES Cyber Systems pretty much how they see fit. This means the SDT must enforce compliance at the device level since the ‘system’ concept is still inconsistent. Provide better examples of what a ‘system’ is and how it can be audited. CIP-007 and CIP-010 require verification of things like ports open, software versions, and logging that can only be checked at the asset level, not the System Level.

Likes 0	

Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the assumption of the SDT that auditors have been expecting entities to demonstrate compliance at the device level. We recommend that greater efforts be made so that a measure will support/reinforce the level of control set forth in the requirement. Secondly, we feel that more coordination between a standard drafting team and auditors may be beneficial. In some instances, a standard could be audited differently than what an SDT had intended. Perhaps auditor representation, or SDT members that have audit experience may be beneficial to have on an SDT as well.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
The present definition of BES Cyber System is very broad, as it is a grouping of BES Cyber Assets to perform one or more reliability tasks. As a result, Responsible Entities have been observed to implement this definition in many ways, from the one-to-one mapping of BES Cyber Assets into BES Cyber Systems to the other extreme of grouping all BES Cyber Assets at one impact level into a single BES Cyber System. This wide range of implementation has made evidence sampling at the BES Cyber System level impossible, forcing audits to focus on BES Cyber Assets rather than on BES Cyber Systems. Also, the term “reliability tasks” has not been defined, and this appears to contribute to the variety of groupings of BES Cyber Assets into BES Cyber Systems. If the concept of the BES Cyber System is to become truly useful, the definition must be modified such that the BES Cyber System becomes a small grouping of BES Cyber Assets that performs a specific function. It may be beneficial to identify a list of functions performed at each type of physical asset, Control Center, substation, and generator. A starting point for such a list can be found in the NERC CIPC document, “Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets,” dated June 17, 2010. While obsolete for the current Standards, this document provided an extensive list of the types of functions performed at each physical asset.	
Likes 0	
Dislikes 0	
Response	

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

Recommendation to make the virtual machine subject to the same requirements as a physical asset but allow deployment to be done in a virtual environment.

PSEG also supports Edison Electric Institute's comments.

Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	Yes
Document Name	

Comment

We agree with the assumption. This may be the expectation of an auditor. However, more education and guidance may be required for auditors to fully understand the technology being used by industry and how to appropriately audit it.

The requirements do allow protections to be performed at a BCS level. There are some requirements where it is easier to apply a control at a BCS level. This would include malware protection at the BCS level, patch assessment at the BCS level, and event logging at a BCS level. Conversely, there are some requirements where it is easier to demonstrate compliance at the Cyber Asset level. For us, that includes baseline of assets.

When addressing compliance with virtual systems, it will be important to have the controls allowed at the host or template level as long as the entity is capable of showing how the control is inherited by a guest.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

Requirements and controls should be still enforced at a BES Cyber System level, but evidence should be provided at a device level. In virtualization and Software Defined Data Centers infrastructure is typically policy driven, meaning IT Engineers specify the ways systems should work via configuration files that apply to all systems within that container. Virtualization in particular adopted this methodolgy very early on in deployment. Therefore, applying rulesets at a system level (i.e.: All Hypervisors must require vendor-signed installation packages) makes sense -- we would want all nodes of the cluster to operate the same. However, evidence should be gathered at the device level (i.e.: provide evidence that hypervisor Cluster01-Node5 only allows vendor-signed installation packages). NIPSCO OT has already taken this stance and it seems to be the best way to manage and maintain compliance.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	Yes
Document Name	

Comment

This is an ongoing problem that extends beyond virtualization. The SDT could consider using the Applicable Systems column to address distinctions between BES Cyber System application of requirements and BES Cyber Asset application on an explicit and per requirement basis.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	Yes
Document Name	

Comment

Southern Company agrees with the SDT assumption. Version 5 introduced the BES Cyber System concept; however, for most of the high and medium impact requirements, auditors expect Responsible Entities to demonstrate compliance at the device level rather than the system as a whole. To address this issue, the SDT could add system-level implementation examples to the Guidelines and Technical Basis along with new system-level evidence examples to the measures of the requirements. Southern agrees that the current standards have a “everything is a Cyber Asset and all requirements apply to all devices” framework which can present numerous issues when applied to the seemingly endless variety of programmable electronic devices in the entire Bulk Electric System. The “per device capability” phrasing helps but often requires research and documentation to prove the negative in its own right.

The current CIP V5 standards allow for the implementation and documentation for virtualization. However because some features of virtualization are not clear, additional guidance should be considered for the implementation of mixed virtual environments, hardware pooling, and temporary virtual machines.

Likes 0

Dislikes 0

Response

Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC

Answer	Yes
Document Name	

Comment

This would require extensive changes in how auditors are sampling for audit. It would also require a look into how CIP-002 is currently defined and applied. CIP-002 talks about identifying the BES Cyber Systems, which consist of BES Cyber Assets. This is has been the explanation given to me about why auditors like to see evidence at the Cyber Asset level.

Likes 0

Dislikes 0

Response

Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

ACES does believe the current standards are designed at the BES Cyber Asset or device level. The CIP standards were created to protect industrial controls systems that impact the BES within 15 minutes. Virtualized machines are not designed with those cyber systems in mind. How can an auditor audit a virtual system that exists in one minute and is gone the next? The two worlds, assumption and architecture do not mesh well, if at all. We would like to see a completely new set of standards that reflect the intangibles of virtualization, storage and networking without being tied to 5 year old definitions and concepts of NERC CIP.

Likes 0

Dislikes 0

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	Yes

Document Name	
Comment	
Reclamation recommends that definition of cyber asset be modified to include hardware, software, data and services.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG agrees that much of CIP is implemented and audited at the individual asset or device level. However, it is not unreasonable to have both a device level and a system level focus. Indeed, device level inadequacies are often mitigated by system level compensatory measures. SDT should continue to allow flexibility in how some risks are addressed where either level might be appropriate. In addition, it may be useful to consider introducing another level for virtualization host resources to address the systemic risks they introduce, as touched on in later responses.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Where it may be a technical incapability to implement required controls on an individual device, the SDT could continue to use the “Per Cyber Asset Capability” language to give entities the flexibility to implement/leverage system-level controls. ATC also agrees with EEI member comments that the SDT could add system-level implementation examples to the Guidelines and Technical Basis along with new system-level evidence examples to the measures of the requirements.	
Likes 0	
Dislikes 0	
Response	

Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
To incorporate virtualization and address the V5TAG transfer issue to clarify the meaning of the term programmable in the current definition of Cyber Assets, the SDT is proposing changes to the definition that include defining the term in the singular rather than the plural. Updating the definition to include virtual environments allows the definition of other terms based on Cyber Asset, such as Electronic Access Control or Monitoring Systems (EACMS) and Protected Cyber Asset (PCA) to also include virtual environments. The proposed Cyber Asset definition is: Redlined ProgrammableAn electronic devices (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in those devices the device. A virtual machine is itself a distinct asset from its host(s). Clean An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
The language should be rewritten to accommodate the different nuances virtual technology presents. Especially concerning the differences between a physical desktop (device level), a standalone virtual desktop (device level), and virtual linked-clone pools (system level) which contain a virtual base/parent image and their linked clones (cloned children images). The requirement is written such that the auditors are bound to look at the System Level, but all of the standards have to be applied at the device level. Ultimately the choice should be up to the entity to define how they want to set up their Virtual Environment as long as all of the security controls are in place.	
Likes 1	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

Version 5 introduced the BES Cyber System concept; however, for most of the high and medium impact requirements, auditors expect Responsible Entities to demonstrate compliance at the device level. To address this issue, the SDT could add system-level implementation examples to the Guidelines and Technical Basis along with new system-level evidence examples to the measures of the requirements.

Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

The concept of the BES Cyber System, to be useful, must be developed further. There needs to be concessions given for protection of a system when the particular requirement can't or isn't implemented on each individual cyber asset. PacifiCorp would support this development in the CIP standards, however does not believe that it is necessary in order to implement language in the CIP standards that support virtualization.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	Yes
Document Name	

Comment

Kansas City Power and Light supports Edison Electric Institute's Comments.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6

Answer	Yes
Document Name	

Comment

Austin Energy (AE) agrees the SDT ***assumes*** most auditors *expect* entities to demonstrate compliance at the device level. However, AE is troubled by the fact we are making *assumptions* about any NERC Standard. To address the inconsistency, NERC should revise the CIP Standards to say what is intended rather than relying on assumptions.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro

Answer	Yes
Document Name	

Comment

Clarify the language of the standard requirements to explicitly indicate where evidence is expected to be provided on a per device/BES Cyber Asset basis as opposed to a BES Cyber System basis or where either or is acceptable and the conditions under which it is acceptable. This is currently left to the auditing entity to communicate and express their audit approach and can lead to confusion and misinterpretation of standard requirement implementation on behalf of entities.

Likes 0	
Dislikes 0	

Response

Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	Yes
Document Name	

Comment

Version 5 introduced the BES Cyber System concept; however, for most of the high and medium impact requirements, auditors expect Responsible Entities to demonstrate compliance at the device level. To address this issue, the SDT could add system-level implementation examples to the Guidelines and Technical Basis along with new system-level evidence examples to the measures of the requirements.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

AZPS agrees with the SDT’s assumption that most auditors expect entities to demonstrate compliance at the device level and that it can introduce inconsistencies in the treatment of physical or virtual assets. However, AZPS respectfully submits that there are additional areas of potential inconsistency that would need to be evaluated and addressed (where determined necessary). AZPS identifies the following areas of inconsistencies for the SDT’s consideration:

- Potential for inconsistent language between the Requirement and associated Measure;
- Potential for inconsistency in audit approaches between regions and/or regional audit staff and the audit documentation utilized during a registered entity’s audit, e.g., interpretation of RSAW “blue notes,” use of sampling tools and methods, etc.; and
- Potential for inconsistency between the language of the Requirement and associated Measure and the audit approaches, as discussed above.

All of these areas of inconsistencies must be considered by the SDT as the addition of virtualized devices has the potential to significantly complicate both compliance and audit approaches and, without clarification regarding these, inconsistencies could introduce complexity, ambiguity, and inefficiency. For example, where a requirement is applicable to a virtualized system, will each component of that system be evaluated or will the system be evaluated at the system or “common” platform level. Additionally, where such systems communicate with external networks or devices, there will need to be a common understanding of how compliance will be evaluated as controls may be “common” under certain configurations and, therefore, applied at the management plane for distribution across all data planes. For these reasons, AZPS recommends that the SDT evaluate each of these potential inconsistencies as it moves through the standards drafting process to minimize the potential for ambiguity and inconsistency by and between both registered and regional entities relative to the demonstration of compliance and the methods and documentation for compliance monitoring.

All of these areas of inconsistencies must be addressed by the SDT to ensure that both registered and regional entities have consistent understanding of the demonstration of compliance and the methods and documentation for compliance monitoring.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	
Document Name	
Comment	
LCRA Transmission, Segment 1, has no opinion at this time.	
Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees implementation of the CIP Requirements are at the BES Cyber Asset or device level. The BES Cyber System concept is just a logical grouping; by definition a BES Cyber System is “***One or more BES Cyber Assets*** *logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity*.” There are no inconsistencies to address, a BES Cyber System is a logical grouping, and you cannot apply the CIP Standards to a logical grouping without knowing what the BES Cyber Assets are.	
Likes 0	
Dislikes 0	
Response	

2. The SDT proposes that each virtual machine and hypervisor are separate Cyber Assets. Do you agree with this position? Please provide a rationale to support your position.

(Refer to the Unofficial Comment Form for more information on this question)

Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC

Answer	No
Document Name	

Comment

The answer to this question is no since a hypervisor is defined as software that allocates resources to VMs. Therefore, a hypervisor should not be a Cyber Asset. The hardware running the hypervisor software should be labeled as a Cyber Asset. This distinction should be clear for all future requirements. Virtualized hardware (VM), and its associated OS, should be classified as Cyber Assets.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	No
Document Name	

Comment

The hypervisor’s host machine and the virtual machine are the separate Cyber Assets. The hypervisor is computer software or firmware that creates or runs the virtual machine, but does not have its own OS or system to enforce CIP controls, similar to a SCADA application running on a server. With regards to protecting the hypervisors, controls should be implemented on the host machine.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

The new definition does not address a Cyber Asset with virtualized storage which should be treated as separate Cyber Assets. The definition offers no guidance for identifying virtual Cyber Assets. A methodology is required for example, start with the function performed, then identifies each component –

Virtual Machine, storage, host and hypervisor using a high water mark. The proposed definition uses the term “[A virtual] electronic device”. A virtual Cyber Asset is not an electronic device, or a device at all. A function, for example providing control of a BES element, could be completed by a software program that runs on a vitual operating system (OS). This virtual OS is its self software, the operation of which is controlled by a hardware hypervisor. The vitual system does not function on its own, the identification of components of the system must be addressed by the standard. Managing each component can be done separately.

The definition does not address how to handle a hyper converged environment where building blocks can include storage, network compute and memory resources.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG disagrees with this proposed definition because it would cause any removable storage device to qualify as a programmable electronic device (“stored operating system” could make the definition more clear).

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE does not agree with the SDT’s proposal to treat each virtual machine and hypervisor as separate Cyber Assets. The hypervisor (parent) is the device or software which runs the virtual machine (child). The virtual machine (VM) cannot operate without the hypervisor. This shared relationship means that neither can be separate Cyber Assets. For example, if a VM has been identified as a BES Cyber Asset (BCA); the hypervisor that runs the VM is also a BCA; which also applies to PACS, EACMS, and PCA’s

Treating the VM and hypervisor as separate Cyber Assets can cause mixed-trust virtual environments; the hypervisor runs CIP and corporate VM’s. CIP controls are only being applied to the CIP VM and not the hypervisor; even though the hypervisor “*if rendered unavailable, degraded, or misused*” can impact the CIP and corporate VM’s.

Likes 0	

Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that each virtual machine and hypervisor are separate Cyber Assets. To ensure clarity, AZPS asserts that virtualized assets, if represented by physical hardware, would meet the current definition of Cyber Asset. Thus, simply virtualizing these assets does not change their criticality or role in the operation of the BES and, as such, these virtualized assets should still meet the definition of Cyber Asset. Moreover, hypervisors running on hardware that manage the resources for virtualized Cyber Assets would also meet the definition of Cyber Assets. Without these physical Cyber Assets, the virtualized Cyber Assets cease to exist. Because these virtualized assets can be identified, classified, and evaluated as Cyber Assets, AZPS strongly recommends that the SDT consider opportunities to modify the existing CIP requirements to expand or clarify that their applicability extends to virtual AND physical Cyber Assets. AZPS understands that there may be some requirements that will not directly apply, e.g., CIP-007-6 R1, Part 1.2's physical port protection requirements would not be applicable to virtualized Cyber Assets. Nonetheless, because these virtualized assets meet the definition of Cyber Asset, they have similar capabilities to meet the majority of the current requirements language. Thus, review and revision to the existing requirements would allow the requirements applicable to all Cyber Assets (based on capability) to be consolidated, which would reduce the potential for confusion and ambiguity given the physical and virtualized nature of virtualized devices and increase the likelihood for the application of consistent approaches by both Regional and Registered Entities.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
NV Energy agrees that each hypervisor and virtual machine are separate Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes

Document Name	
Comment	
Based on modifications to the definition of Cyber Asset, each host and virtual machine can be separately managed and, therefore, should be distinct Cyber Assets. However, AE finds the use of the term "host" problematic when used in connection with a virtual machine. Host is very general and typically refers to servers and systems. AE would recommend using the following definition: An electronic device (physical or virtual) with its operation controlled by a stored program which the end user can change or replace and includes the hardware, software and data. A virtual machine is itself a distinct asset from its hypervisor-host.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Kansas City Power and Light supports Edison Electric Institute's Comments.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
The controls and risks apply individually to each virtual machine as well as the host (and hypervisor if considered the host).	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI agrees that a virtual machine is distinct from a hypervisor. The guest machine or virtual machine is what the hypervisor manages/controls on a host machine. Host machines are another distinct component in the virtualization environment; however, we have found that the host (or VM host) and hypervisor may be used interchangeably or the hypervisor term may include the host machine. It would be helpful for the SDT to clearly define these terms so that all Responsible Entities, the ERO, and other stakeholders are using the same meaning for each term. A common lexicon that can be applied to all virtual or logical technologies will be required to enable all stakeholders to understand the concepts being presented by the SDT.	
Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
This clarifies, the definition of the term *programmable*. See note above about the flexibility of what is a virtual machine. The entities should be allowed to define how they setup their virtual environments. We agree with the first sentence and how it is defined. The second sentence should be modified to allow the entities to determine whether the Hypervisor and its children are a BES Cyber Asset or multiple BES Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
While this distinction may help to alleviate confusion, virtualization is a complex subject where incorrect or interchangeable use of these technical terms could lead to misinterpretation. ATC recommends that the SDT consider providing additional clarity around these terms through guidance and examples without officially them. ATC recommends that the SDT resist the temptation to reinvent/redefine these terms as historically this approach had the	

unintended consequences of creating ‘new terms’ that are too prescriptive, do not scale to ever-changing technology, and/or contradict or otherwise render commonly acceptable technological terms moot.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

- Agree that “virtual machines” should be treated as separate cyber assets because applying the CIP requirements to “host devices” without recognizing that “virtual devices” are, in actuality, being managed as individual logical devices is fundamentally counterproductive and introduces many artificial, confusing, and unnecessary dilemmas.

- However, special consideration likely should be given to “host devices” as they represent a new systemic risk to potentially many hosted, dependant BCSs.

- Furthermore, the real risk of virtual machine “escape” attacks (ref: https://en.wikipedia.org/wiki/Virtual_machine_escape) is difficult to address but should be acknowledged. Virtualization discussions presented so far have not mentioned this low probability but very high impact risk. A successful such attack would put at risk all virtual assets in the host environment at once by taking control of the virtualization manager (or CMS). In light of this new, elevated risk, should it be acceptable, for instance, to host “non-CIP” virtual machines on a host shared with CIP virtual machines? It might be advisable, for instance, to deem “non-CIP” virtual assets as PCA equivalents unless some agreed upon mitigating measures are met to better protect the host devices and manager. An example of such a measure might be having the CMS non-virtualized and protected by non-virtual firewalls (i.e. The CMS would not be self-hosted). This is similar to separation of management and data planes addressed in question 7, however either variation might not be sufficient to mitigate these virtual machine escape attacks.

- As a minor matter of terminology, the “hypervisor” is more akin to an operating system and not the actual physical host hardware. As such, use of terms such as “host device” or “host cyber asset” would be more appropriate in the question wording than “hypervisor”.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	Yes
Document Name	

Comment

Reclamation supports the view of the SDT. The security required for a hypervisor is not necessarily the same as the security required for virtual machines because they are separate cyber assets.

Likes 0	
Dislikes 0	

Response

Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

Yes, if they can be tracked and monitored by a naming convention. Each name of the virtual machine or hypervisor is an instance. If you were to rationale out that a function being performed is a Cyber Asset, the list would be impossible to manage.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	Yes
Document Name	

Comment

Southern Company agrees each virtual machine and hypervisor are separate Cyber Assets. The purpose of the hypervisor is to manage one or more virtual machines. Virtual machines provide the same functionality of a physical computer or a Cyber Asset. Since many of the CIP requirements are at the device level, we view each instance of an OS as its own Cyber Asset and we agree it is not simply a disk image data file or application.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	Yes
Document Name	

Comment

The SDT should consider the hypervisor and overlying virtual machines as separate Cyber Assets to enable consistent and distinct protections to be applied in each case.

Likes 0

Dislikes 0

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

The virtual machine represents a separate and unique attack surface from the underlying hypervisor and therefore needs to be protected as a distinct asset. Treating the hypervisor and guest virtual machines as a single device confuses physical and virtual domains and doesn’t make sense from a practical standpoint. For example, management of the ports/services of the hypervisor with numerous virtual operating systems running on the same physical hardware becomes very difficult.

Likes 0

Dislikes 0

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

It is impossible to secure a guest VM and the physical hypervisor using the same technology in a requirement. For example, we would have BIOS firmware to maintain on the hypervisor. We do not have that in a virtual machine. Likewise, there are security updates for Windows guest Operating Systems that is updated much more frequently than the hypervisor -- however a vulnerability in the guest operating system does not impact the host hypervisor, and therefore it is critical to treat the two as separate entities. NIPSCO OT has always considered the hypervisor and the guest VMs as separate entities even under CIP Version 3.

Likes 0

Dislikes 0

Response

David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Based on the modifications provided to the definition of Cyber Asset, each host and guest can be separately managed objects and therefore should be treated as distinct Cyber Assets.	
Likes 0	
Dislikes 0	
Response	

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG supports Edison Electric Institute’s comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy recommends that the drafting team consider whether a definition of “system” may be necessary. Depending on the type of language that is used in revising the standard language, a consistent and industry wide definition of the term “system” could remove some ambiguity which may exist.	
Likes 0	
Dislikes 0	
Response	

Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	

Answer	Yes
Document Name	
Comment	
VMs and Hypervisors have separate Security Controls. In addition, the processors that manage the storage arrays must also be considered separate Cyber Assets as well. So you effectively have three cyber asset considerations with regards to virtualization: Virtual machine, Hypervisor, and Storage processors.	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
There are very few protective measures that can be taken at the hardware or virtualization host layer that don't ignore the individual components of the multitude of operating system environments residing on the physical asset. This gets even more complex as modern standards, such as containerized applications, become prevalent - something the SDT will need to address very soon or risk the standards becoming obsolete to current technology.	
Likes 0	
Dislikes 0	
Response	
Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Based on the modifications provided to the definition of Cyber Asset, each host and guest can be separately managed objects and therefore should be distinct Cyber Assets.	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
Answer	Yes
Document Name	
Comment	
The SDT should consider the hypervisor and overlying virtual machines as separate Cyber Assets to enable consistent and distinct protections to be applied in each case.	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
SCE&G treats a virtual machine and a hypervisor as separate devices. Each device has to be configured, applied patching, etc.	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
The SDT should consider the hypervisor and overlying virtual machines as separate Cyber Assets to enable consistent and distinct protections to be applied in each case.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	

Answer	Yes
Document Name	

Comment

AEP recommends the lead-in sentence be reworded as follows, “The SDT proposes that each virtual machine and host are separate Cyber Assets.” The hypervisor is a piece of software running on the host and serves as an abstraction layer between the virtual machines and their physical host. Accounting for physical hosts and virtual machines separately is appropriate as they are often managed and supported as separate entities.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

You must consider both the hypervisor and each virtual machine as separate assets as each has a defined purpose and operation separately.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	Yes
Document Name	

Comment

For some common virtualization platforms (VMWare, XenServer), there appears to be clear separation between the host OS and guest OS’s. This is evidenced by the ability to update the hypervisor OS and VM OS’s independently of each other. However, this does not preclude a design existing where there is much tighter integration between the Host OS and Guest OS’s which blurs any separation. Also any system in which VM’s are dynamically created and destroyed based on workload (e.g. dynamic provision) could complicate treating each VM as a distinct asset as opposed to an instance of an application.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
This proposal seems reasonable, although a systems-based approach may eliminate the need for such differentiation.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST believes this position is consistent with a widely (multi-industry) accepted view of virtualization that considers each so-called “guest OS” to be separate and distinct from the underlying hypervisor and its host OS. N&ST believes the draft NIST Special Publication, “NIST Definition of Microservices, Application Containers and System Virtual Machines,” SP800-180 (DRAFT) also supports the SDT position.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Hypervisors offer complete dataplane (network and operating sytem-level) separation from their hosted virtual machines. The hypervisor and virtual machine each run an independent operating system, and all process and memory allocations are contained within their respective operating systems.	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy considers a hypervisor distinct with an independent operating system, software, user access list, network address, security configuration, etc from its guests.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The virtual machine and hypervisor are managed as separate devices and act as separate devices and should be treated as such.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Any device that communicates should be considered a separate cyber asset. For example, the host physical machine that has an installed hypervisor would have ethernet interfaces for the hypervisor as well as interfaces for the virtualized devices. The virtual machines could be connected to a virtual switch which is connected to the physical Ethernet interface of the host/hypervisor machine. Therefore, any device that communicates and performs a dedicated function should be considered a separate cyber asset.	
Likes 0	

Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Each VM and each hypervisor exist as separate network-connected devices, so this approach makes sense.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Yes, Exelon agrees that when implementing a virtualized environment for CIP, the VM Host machine(s) as well as each individual VM guest should be considered as distinct Cyber Assets. We believe the term “VM Host machine(s)” should be utilized instead of “hypervisor” to identify what in a virtualization environment requires CIP Protection in addition to the individual VM’s.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Please reference the response provided for #3.	
Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

BPA agrees that the proposed definition of Cyber Asset must include virtual machines (see caveat in question 3 regarding "data inside the device"). BPA believes that both "virtual machine" and "hypervisor" are well-understood terms with formal definitions (NIST SP 800-125, SP 800-125A {Draft}, SP 800-125B) and broad IT Industry acceptance, thus do not need further definition in the NERC Glossary. BPA agrees that each Hypervisor and Virtual Machine is a distinct Cyber Asset. Controls and strategies for securing virtual machines across a variety of industries have been published by agencies such as NIST and SANS.

The key issue the SDT appears to address in this revised definition is clarifying the scope or boundaries of a given virtual cyber asset in order to apply requirements and controls to each. Clarifying the definition is only necessary to address gaps in current requirements language that allow for miss-applying the requirement. BPA believes Industry understands and can securely apply the technical controls.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	

Comment

On a network subnet, a virtual machine is logically an independant Cyber Asset (node) and should be afforded the appropriate CIP controls based on its Applicable System catagorization.

Likes 0	
Dislikes 0	

Response

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

3. Do you agree that the proposed Cyber Asset definition clarifies the term *programmable*? Please provide a rationale to support your position.

(Refer to the Unofficial Comment Form for more information on this question)

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA agrees that the SDT's proposed definition of *programmable* encompasses a device subject to hardware and software changes by the end user.

However, BPA disagrees that the definition should apply to the data stored in the device.

- Data inside the device is peripheral and irrelevant to the operation of the device.
- The use of *data* in the current definition of *Cyber Asset* does not match Section 215 of the Energy Policy Act of 2005 that reads: "…programmable electronic devices and communication networks including hardware, software and data **that are essential to the reliable operation of the bulk power system**."
- Best practice IT Security across a broad spectrum of industries typically separates the mechanisms of protecting a *system* (better known as *Information Assurance,* Source: NIST SP 800-50, CNSSI-4009) from the mechanisms of protecting *data* transiting or resident on that system (the latter being *Information Security,* Source: NIST SP 800-59; SP 800-53; SP800-53A; SP 800-60; CNSSI-4009; FIPS 199; 44 U.S.C., Sec. 3542).
- The introduction of the concepts of *management plane* and *data plane* which are referenced in question 8 is a useful addition to the NERC CIP discussion because it enables appropriate controls to specifically protect systems or data.

Likes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

Dominion does not recommend a change to the current definition of Cyber Assets. If a change to the definition is made, Dominion recommends using the more generic term “logical” instead of “virtual”, as outlined below. The term “logical” would encompass any virtual environment including dual-bootable OS machines. Additionally, the phrase, “*including the hardware, software, and data in the device* “ is misplaced and should be moved. Finally, Dominion proposes that the term “machine” should be replaced by “device” for consistency:

Recommended language change:

“An electronic device (physical or virtual logical), including the hardware, software, and data in the device, whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual logical machine device is itself a distinct asset from its host(s).”

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

Exelon does not agree that the proposed update to the Cyber Asset definition sufficiently clarifies the meaning of “programmable.” The addition of the language “a stored program that can be changed or replaced by the end user” can be interpreted to extend the scope of the CIP requirements down to all field-updateable devices. This includes chipsets that are configurable but not programmable. If changing the device requires physical removal of a chip or any other disassembly or destruction of the device to change or update the device, then the device should be categorized as “not programmable”.

The CIP-002-5: BES Cyber Assets Lessons Learned published by the NERC CIPV5 Transition Program provides examples of what the study participants used to address “programmable” during the implementation of the CIPV5 standards. Specifically, page 3 states: “study participants set the scope to be evaluated as those devices that have a microprocessor and can accept firmware, software or logic. Additionally, the study participants considered devices that had a physical or wireless port or a web interface that can be used to “flash” firmware to be Cyber Assets and then evaluated them to determine whether they meet the BES Cyber Asset definition.”

Since the term “Cyber Asset” is foundational to the entire suite of CIP Standards, Exelon is concerned with the removal of the word “programmable” and changes to the Cyber Asset definition unnecessarily prompting an entire reassessment of our Cyber Assets. Exelon has an internal definition of “programmable” that is consistent with the BES Cyber Asset Lessons Learned and encourages the CIP SDT to use a similar approach. If the CIP SDT determines to make adjustments to the Cyber Asset term, any updates to clarify “programmable” should make use of example statements that are consistent with the published Lessons Learned and not replace the word “programmable” within the Cyber Asset definition.   Additionally, Exelon would support the addition of a statement to the Cyber Asset definition that clarifies that “A virtual machine is itself a distinct Cyber Asset from its host(s).” Exelon does not believe that it is necessary to add the parenthetical reference “(physical or virtual)” to the Cyber Asset definition.

Likes 0	

Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF

Answer	No
Document Name	

Comment

PJM suggests removing “by the end user.” A stored program that can be replaced or updated “by the end user” does not take into account the principle of least privilege. End users should not have the ability to update software, but rather to only perform system functions relevant to their roles. For example, a server is a programmable device, but the operating system software and firmware cannot be updated by end users – only by system administrators.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP requests additional clarification of *stored program*. The phrase “including the hardware, software, and data in the device” is unnecessary. Replacing the final sentence of the proposed definition with, “A virtual device is a Cyber Asset” would add clarity.

SRP also requests clarification on dip switches and jumpers. Under the proposed definition would it be acceptable to exclude devices that are configured using dip switches and/or jumpers as cyber assets?

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy believes the proposed Cyber Asset definition does not clarify the term programmable and is not clear where "data in the device" is concerned. In a virtual environment, the data accessible to a virtual machine (VM) is still "in" the hypervisor, but not accessible to it. Data stored on a storage area network (SAN) may not be accessible to the administrator of the SAN, but only authorized users of the SAN. CenterPoint Energy believes the clause "including hardware, software, and data in the device" does not add value and clarity to the Cyber Asset definition and should be removed.

As an alternative, CenterPoint Energy recommends addressing data that is either a) accessible by an authorized user of an asset; or b) data that is impacted by the availability of an asset, but not accessible to an authorized user of that asset. The latter case could be data stored in a VM or container that can be made unavailable by actions of the hypervisor administrator, but is not accessible or modifiable by the administrator. Data that is not accessible to users of a device cannot be modified by programmable instructions, and therefore might be excluded from the definition.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

Modifications to the definition of such a key term can have far-reaching and potentially unforeseen consequences. Modifications to the definition of “Cyber Asset” could impact all aspects of an entity’s CIP compliance program. AEP suggests the following wording for the definition of Cyber Asset: “An electronic device (whether physical or virtual, including […]) whose function is controlled by an end user created stored program. A virtual machine is itself a distinct asset from its host(s).”

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Programmability sould be seen as independent of who perform the action.

Do you consider program configuration and scripting (scripts) as part if this definition?

We think that program configuration and scripts be part of the term parameterized.

We found a definition for Script: A computer script is a list of commands that are executed by a certain program or scripting engine.

We suggested to modify the definition of programable for :

An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed, replaced ***or parameterized*** *by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).*

Likes 0	
Dislikes 0	

Response

Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6

Answer	No
Document Name	

Comment

The phrase ***controlled by a stored program*** is problematic and will lead to no more clarity than the use of the word programmable.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG disagrees with this proposed definition because it would cause any removable storage device to qualify as a programmable electronic device (“stored operating system” could make the definition more clear).

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE

Answer	No
Document Name	

Comment

Prefer leaving the use of the term “programmable” this definition as is. Entities may have an internal definition in their existing CIP compliance program. Changing this foundational concept has multiple far-reaching impacts. Modifying the Cyber Asset definition to address scripts and firmware is unnecessary since they are already covered in CIP-010. Guidance could be added to CIP-002 on possible definitions of the term “programmable”.

In virtualized environments, the physical infrastructure can be shared between BES Cyber Systems and other non-CIP Cyber Assets while maintaining isolated virtualized environments for each.

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	No
Document Name	

Comment

Creating a definition specific to the CIP standard does not benefit the SDT or the industry. Standards-based language should be used for these kinds of terms, not newly created terms with questionable interpretations. For example, why use the terms "Cyber Asset" and "programmable"? Why not use the dictionary definition of a "Computer" as "an electronic device for storing and processing data, typically in binary form, according to instructions given to it in a variable program", followed by giving specific examples of what the SDT considers to be a "Computer" in scope of the standard?

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not agree that the proposed definition of Cyber Asset helps to clarify the term *programmable*. We believe that there is still the possibility for a difference of opinion between an entity and a regulator as to what an end user is capable of. We recommend the drafting team consider the following as a definition for *programmable*:

“A programmable device has a communication interface through which it’s stored program or configuration may be accessed, verified, modified, or replaced.”

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation

Answer	No
Document Name	

Comment

FirstEnergy does not support any modifications to the Cyber Asset definition because it is foundational to the existing implementation of the CIP Standards. Any change will create a significant compliance exercise that requires burdensome compliance paperwork review and updates with no benefit to the reliability of the BES. Instead of modifying definitions, the SDT should seek to add requirements, guidance, and measures to enable the secure use of virtualization in the CIP environment.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

While the change does help clarify the term “programmable,” other issues have been introduced. In addition, the phrase “that can be changed or replaced by the end user” is both ambiguous and ill-advised from a security perspective.

The phrase is ambiguous in that it can be construed as broadly as a laptop PC that has been locked down by its administrators so that the end user cannot modify the programming, only the data.

However, even if the definition is changed to something like “a stored program that can be changed or replaced only by direct intervention in the hardware,” this will still leave many devices out of scope. It can be argued that these devices are some of the most risky devices in a Responsible Entity’s inventory, as any programs on these devices cannot be patched even when vulnerabilities are found. As an example, see “https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/”.

Changing the definition of Cyber Asset such that these devices are not included in the required CIP protections, but will be out of scope for the CIP Standards (and thus completely invisible to audit teams) should not be considered acceptable.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

The scope of the revised definition proposed seems more broad than the previous definition. Caution must be exercised to ensure that additional unintended devices, for example ‘smart’ instruments that use HART or similar protocols, are not inadvertently defined as Cyber Assets by a change to the term’s current definition intended only to address virtualization.

PSEG also supports Edison Electric Institute’s and NPCC’s comments.

Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	No
Document Name	

Comment

This definition does not take the distinction between configurable and programmable as was discussed under the V5 project into account. This new definition would seek to include devices that are configurable (i.e. via dip-switches) as changes to these predefined configurations/inputs would result in a change to a stored program by an end-user. Devices that have embedded programming that cannot be changed by end users, except through pre-defined configurations/inputs should be excluded.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Suggest provide guidance or clarification to include software / firmware in definition of “stored program”.

Likes 0	

Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
Prefer leaving the use of the term “programable” in the definition as is. Entities may have an internal definition in their existing CIP compliance program. Changing this foundational concept has multiple far-reaching impacts. Modifying the Cyber Asset definition to address scripts and irmware is unnecessary since they are already covered in CIP-010. Guidance could be added to CIP-002 on possible defintinos of the term “programable”.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
Southern Company does not agree with the proposed changes to the Cyber Asset definition. The current Cyber Asset definition is an integral part of the the CIP Standards. Modifications to the Cyber Asset definition would require a review of the current compliance documentation for thousands of devices. NERC has provided implementation guidance on defining BES Cyber Assets that Southern finds sufficient regarding the term programmable. The SDT should add guidance, and measures to enable the secure use of virtualization in the CIP environment.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	

I don’t think it is clear as to how that included virtualization. Is a virtualized storage device, programmable? Trying to fit virtualization concepts into Cyber Assets that are tangible is problematic. I would recommend using a NIST Virtualization Guidance and have two set of standards. That perform functions in different way, terminology and capabilities.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends that definition include programmable electronic devices, including the hardware, software, and data that is essential to the reliable operation of the bulk electric system.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI does not support any modifications to the Cyber Asset definition because it is foundational to the existing implementation of the CIP Standards. Any change will create a significant compliance exercise that requires burdensome compliance paperwork review and updates with no benefit to the reliability of the BES. Instead of modifying definitions, the SDT should seek to add requirements, guidance, and measures to enable the secure use of virtualization in the CIP environment.

Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	

Response

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No

Document Name	
Comment	
SCE does not support modifications to the Cyber Asset definition because of its impact to the current CIP standard implementations. Modifications may create potential compliance review and updates with no significant benefit.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Kansas City Power and Light supports Edison Electric Institute's Comments.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
NV Energy does not believe that the proposed definition clarifies the term programmable. A possible alternate definition could be: An electronic device (physical or virtual) that is controlled by a stored program and has a locally or remotely accessible input interface such as a management port or a web interface that would allow the introduction of firmware, software, or a logic update. NV Energy does have some concerns with the changing of the Cyber Asset definition. Because this definition is the foundation to the existing CIP Standards any change will create a significant compliance exercise that requires burdensome compliance paperwork review and updates with no benefit to the reliability of the BES. Instead of modifying definitions, the SDT should seek to add requirements, guidance, and measures to enable the secure use of virtualization in the CIP environment.	
Likes 0	
Dislikes 0	
Response	

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS respectfully asserts that the proposed definition introduces new areas and potential for ambiguity and confusion relative to the term "programmable." In particular, AZPS identified the following questions:

- Where is/can the "stored program" stored?
- Can it be stored on a separate Cyber Asset for the control of a virtualized or different asset?
- Who is the "end user" and how is "changed or replaced by the end user" defined?
- Does such change or replacement have to be performed directly by the "end user" or can it be performed by a third party through a contractual service obligation?
- Does the phrase require that an "end user" have the actual technical or other capability to make such a change or replacement before the asset would qualify as a Cyber Asset?
- If an "end user" has no one on staff that can change the stored program and no service provider, is the asset not considered a Cyber Asset?

Given the potential confusion associated with these questions, AZPS offers the following definition of Cyber Asset:

"A physical or virtual electronic device containing operating system(s), software, and/or firmware which programming and configuration can be modified.

Physical electronic devices include the hardware, software, and data in the device.

A virtual electronic device includes its virtual hardware, software, and data, and is distinct and separate from its physical host(s)."

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	
Comment	
The SDT should consider removing the language "by the end user." The security objective should be to afford controls to a Cyber Asset irrigardless of who can change or replace it.	
Likes 0	
Dislikes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Response	
Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
I also believe that the terminology as to “stored program” offers flexibility in that this can be software or programmable hardware (e.g., as in a field-programmable gate array).	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Removal of the word Programmable narrows the new wording and the definition to software. The term ‘end user’ should be defined to avoid confusion.	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST believes the qualifying criterion, “...stored program that can be changed or replaced…” is helpful.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
A definition in the singular ordinarly is more precise and easier to parse than one in plural. In this case the difference appears relatively minor, with the exception that the added sentence, about a virtual machine, adds clarity about these cases.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
It seems clear from the definition that what is being talked about is re-programmability—the ability for a devices function to be changed, which obviously has cybersecurity implications that a hard-coded, un-alterable device does not. Whether a device is virtual doesn’t seem to alter they fact that it may be re-programmable.	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

The updated definition accounts for the ability to change hardware, software, and data for an asset. This provides for firmware, data, and other software that can change or update the functionality of the device and hence is programmable. This differs from a fixed device that is purpose built to perform one action and cannot change hardware, software, or data to change the functionality.

Likes 0	
Dislikes 0	

Response

Lee Maurer - Oncor Electric Delivery - 1

Answer	Yes
Document Name	

Comment

The definition is an improvement in that it addresses the meaning of programmable and allows for the use of virtual systems instead of just physical systems.

Likes 0	
Dislikes 0	

Response

Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC

Answer	Yes
Document Name	

Comment

We suggest "computing" rather than "electronic". Please give a definition of “end user” that includes administrators. However, I think it is beneficial to retain “by the end user” because this limits the inclusion of additional devices that might not apply because they are not truly programmable as in the ability to be provided with coded instruction for performance of an automatic task either serially or through Ethernet. I disagree with this alternative. I think the 4th alternate example is the best suggestion with the added language regarding the virtual machine.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	Yes
Document Name	

Comment

Clarification is needed that user-modifiable configuration settings are not considered part of the stored program. Also, replace the term “asset” with “device.”

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	Yes
Document Name	

Comment

The definition is an improvement in that it addresses the meaning of “programmable” and allows for the use of virtual systems instead of just physical systems.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

This new definition is significantly clearer and leaves must less room for interpretation. This aligns closely with how NIPSCO OT has deployed virtualization, treating every virtual machine as it's own BES Cyber Asset. **However** I would caution that the SDT somehow accounts for things such as the firmware on a hard disk. Firmware on a disk controls the operations of the drive, which especially in enterprise-grade hardware is certainly modifiable. I do believe it is the intent of the SDT that hard drives, peripherals, etc of the asset are all logically grouped together, providing they're managed together. For example, most of our servers get hard drive firmware as part of the server firmware package. The server as a whole is placed at a certain firmware version, which includes hard drives. I would suggest that if a Storage Area Network was used to store the data for a device the

Storage Area Network device should be maintained separately from the collective BCAs. Hard Drives, IO cards, etc should all be considered part of the same BES Cyber Asset. While this new definition is much clearer, some additional scope restrictions would further reduce confusion.	
Likes 0	
Dislikes 0	
Response	
Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
The proposed definition is much clearer and removed most of the ambiguity around programmable.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Yes, this definition better describes the essence of cyber assets and their malleable nature versus devices whose functionality is permanently set. There is yet some concern that devices that may appear “permanently set” or “non-programmable” might actually consist of common programmable computer architectures “under the hood” and that this might be something of a loophole. If an irresponsible vendor of such a system elects not to disclose the internals of a device and refuses to release updates of any type, then the device could harbor CIP related concerns, elevated for lack of updates, and yet still not qualify as a cyber asset under the proposed definition. This concern might be partially addressed by dropping the words “*by the end user*”.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

While the Cyber Asset definition is foundational to the existing implementation of the CIP Standards, in its current form it does not go far enough to adequately capture the devices that should be under the purview of the standards. ATC supports the revised definition and recommends the SDT consider replacing the word “program” with the word “executable code” for added clarity. The use of the word “program” might may have the unintended consequences of bringing in digital logic based devices.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Yes the standards need to allow for mixed trust devices as long you can logically separate them. The CIP standards need to be modified to support this because currently they do not address this. Not all companies have the resources to have multiple hypervisors for both CIP and Non-CIP.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
PacifiCorp believes that the language does provide some clarity to the term *programmable*, but does not substantially alter the definition. While we believe that we should have a definition for *programmable*, we do not believe that developing one now is required to develop requirements necessary to support virtualization. PacifiCorp suggests a dedicated effort directed at clarifying the language in CIP-002 so that application of the CIP standards becomes more consistent across the industry.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes

Document Name	
Comment	
The revised definition addresses the meaning of "programmable" and allows for using virtual systems instead of just physical systems.	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 1,5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE recommends the following: “*A programmable (able to be provided with coded instructions) electronic device (physical or virtual), including the hardware, software, and data in those devices*.”

Likes 0	
Dislikes 0	

Response

4. In virtualized environments, the physical infrastructure can be shared between BES Cyber Systems and other non-CIP Cyber Assets while maintaining isolated virtualized environments for each.

Such configurations are not addressed explicitly in CIP-005-5. Are modifications required to address the issue? Please provide your rationale.

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The current CIP-005-5 standards do not sufficiently address the logical isolation and separation using VLANs. If you can acknowledge and allow entities to do this, it would be highly beneficial to them and to the auditors. VLAN's can be separated and standards can be applied to allow this separation.	
Likes 0	
Dislikes 0	
Response	

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Standard 5 requirements are clear enough to enable an entity to architect the infrastructure as needed and to segment for subnet isolation.	
Likes 0	
Dislikes 0	
Response	

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	No
Document Name	
Comment	

Agree with the below rationale for question #5.

Concerning virtual networks, network devices can have multiple logical networks configured (e.g. virtual local area networks (VLANs)). Physical or virtual devices perform "logical isolation" when configured such that some network interfaces are available inside an ESP, and other interfaces are outside an

ESP and the two networks cannot communicate with each other inside of the device. This would not prevent the VLANs configured inside the device from communicating through an EAP.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
The premise of the question, “In virtualized environments, the physical infrastructure can be shared between BES Cyber Systems and other non-CIP Cyber Assets while maintaining isolated virtualized environments for each,” is not correct. See “https://cmaurice.fr/pdf/ndss17_maurice.pdf”.	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
No modifications necessary.We do not use.	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	No
Document Name	
Comment	

CIP-005-5 does not need to explicitly address virtualization. The Standard is adequate as written, and allows for the use of virtualized systems within an ESP boundary. Mixed-used virtualization which crosses ESP boundaries is an insecure practice, because any vulnerability in hosted systems can expose networks and host that share the same hypervisor.

We are concerned about scope creep into non-BCA CIP assets, e.g. EACMS. Virtualized EACMS should not inherit the same protections required of BCS.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

AEP recommends the SDT modify the guidelines and technical basis of CIP-005 or other standards to include additional language supporting the hosting of multiple impact ratings on the same Cyber Asset. The impact ratings of BCS comprised, in part or in whole, of virtual Cyber Assets can be independent of the impact rating of the physical Cyber Asset host. Cyber Assets hosting virtual Cyber Assets are assigned the impact rating of the highest impact BCS or highest impact rating EACMS, PACS, or PCA it hosts. A "non-CIP Cyber Asset" hosted on a CIP Cyber Asset would not have an impact rating imparted on it. Responsible Entities should be expected to demonstrate segmentation between virutal Cyber Assets of differing impact ratings. Further, AEP recommends the SDT develop reference architectures accounting for potential use cases.

Likes 0	
Dislikes 0	

Response

Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

I checked “no” on the assumption that the new definition of “cyber asset” would extend to all other existing standards reliant on the definition of “cyber asset”.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

Yes. Assuming that virtualization is permitted for BES Cyber Systems, which AZPS supports, to the extent possible, AZPS recommends revising and/or clarifying through revisions to defined terms that the existing CIP Reliability Standards (such as CIP-005) are applicable to virtualized devices. Additionally, AZPS recommends that the SDT clearly address the following:

- Whether or not non-CIP Cyber Assets are permitted to operate on physical infrastructure used by virtualized CIP Cyber Assets;
- Whether CIP Cyber Assets of different impact ratings are permitted to operate the physical infrastructure used by virtualized CIP Cyber Assets;
- How a Registered Entity should extend CIP-005-5 controls through lower level elements of a virtualization stack, such as a hypervisor or other shared virtualization services;
- Whether, if BCS(s) of different CIP-002 impact ratings reside on the same physical/shared virtualization environment, all BCS would be subject to a “high-water mark” requirement based on the highest impact BCS utilizing the shared environment.

Likes 0	
Dislikes 0	

Response

Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	Yes
Document Name	

Comment

NV Energy feels that additional language in CIP-005 would be helpful to provide guideance as to what methods are considered to be adequate to overcome reisks and provide secure isolation or separation of the environments.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro

Answer	Yes
Document Name	

Comment

The current standard language is not sufficient to clearly differentiate between the boundary of what is in scope for CIP protections and what is not regarding virtualization. Additional explicit language and examples would be beneficial for entities in this regard.

Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
To encourage consistent implementation, modifications would help ensure implementation of proper controls and architecture to reduce risk to BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Kansas City Power and Light supports Edison Electric Institute's Comments.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
While it is a practice that PacifiCorp would likely not employ, modifications to CIP-005 (as well as possibly CIP-002, CIP-007, and CIP-010) would be necessary to support mixed-trust environments.	

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	

Response

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SCE believes that clarification is needed on the classification of the shared asset. For example, will non BES-assets come in scope due to common physical infrastructure? SCE recommends that virtualization implementations used for CIP Cyber Assets should not share physical infrastructure with non-CIP Cyber Assets.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

If the intent of the SDT is to allow sharing of physical infrastructure between CIP and non-CIP Cyber Assets through virtualization, then new requirements would need to be added to ensure adequate isolation methods are implemented. For example, virtual technologies cannot deny access by default as required by CIP-005-5, Requirement R1, Part 1.3. Currently, virtualization is used for CIP Cyber Assets, but these implementations do not share physical infrastructure with non-CIP Cyber Assets.

Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	Yes
Document Name	

Comment

ATC recommends the SDT consider potential unintended consequences and construct the requirement in a manner so as to preclude regional interpretations of high watermarking to result in rendering the added flexibility moot. Additionally, the requirement must address what constitutes an EAP where and ESP dissects physical infrastructure Additionally, ATC support EEI's comments that new requirements would need to be added to ensure adequate isolation methods are implemented. For example, virtual technologies cannot deny access by default as required by CIP-005-5, Requirement R1, Part 1.3. Currently, virtualization is used for CIP Cyber Assets, but these implementations do not share physical infrastructure with non-CIP Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
There is the concern, as raised in response 2, of "escape attacks", which it might be appropriate to acknowledge or address in part or in full in CIP-005. As discussed in response 2, it may be prudent to require more stringent risk mitigation approaches before allowing mixing of CIP and non-CIP Cyber Assets on a shared host resource or else all otherwise non-CIP virtual assets would be held to the PCA requirements. It would perhaps be advisable to explicitly state that all virtualization host devices which host CIP virtual BCAs would in turn be classified as BCAs. This could tie in with the idea of a third level to complement the device and BCS levels as discussed in response 1 and 2. Finally, in the case of software defined network "switches" that reside completely in the virtualization platform as an instantiated component of that platform, it is currently unclear if that would be regarded as a separate virtual cyber asset, as would be the case with a virtual machine or physical switch. In many cases these virtual networking components aren't managed in a way that's analogous to their physical counterparts (no user accounts, passwords, patching, etc.) because they are managed entirely in the "management plane". Do they need be treated as a distinct virtual asset?	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Reclamation recommends adding virtualization to the current CIP-005-5 as it relates to the OSI Model.	
Likes 0	

Dislikes 0

Response

Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

Yes they need to be addressed through a virtualization standard and not forced into the current CIP concept.

Likes 0

Dislikes 0

Response

Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC

Answer	Yes
Document Name	

Comment

We would need language that states we can use infrastructure to support protected and non-protected areas. Based on current CIP-005 language, it seems that we cannot use protected hardware/infrastructure to service a larger environment (i.e., regulated and non-regulated). We do not believe that the same rigor should be required of the supporting infrastructure. There should be a tiered approach where the Cyber Assets running the critical services receive the most attention.

Likes 0

Dislikes 0

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	Yes
Document Name	

Comment

Southern Company agrees modifications to CIP-005-5 are needed to address sharing physical infrastructure between BES Cyber Systems and non-CIP Cyber Assets in virtual environments. Additional requirements could be considered to ensure isolation methods are implemented when virtual environments are shared. Current approaches are to avoid mixing CIP and non-CIP environments until further clarity can be provided through the Standards development process.

Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	Yes
Document Name	
Comment	
From the CIP compliance standpoint, one of the reasons to isolate virtualized environments, whether physical or virtual, is to allow for different impact level for each environment. It is unclear at this time, the SDT's intent in allowing mixed mode configurations. As currently written, CIP-005-5 requires all components contained in a virtual system to be protected at the impact level of the highest single component of the system. CIP-005-5 would need to be revised to allow for mixed impact levels within a single virtual host.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
The ESP definition is defined as a logical border but there is currently no construct by which to apply layer 2 network controls for logical isolation to support this type of configuration. All controls are applied at Layer 3 for an ESP at the EAP.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	

To ensure consistency of implementation, modifications would help ensure that proper controls and architecture are implemented to reduce risk to BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

From the CIP compliance standpoint, one of the reasons to isolate the virtualized environments, whether physical or virtual, is to allow for different impact level for each environment. It is unclear at this time, the SDT's intent in allowing mixed mode configurations.

PSEG supports Edison Electric Institute's comments.

Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy agrees that the current CIP standards do not explicitly address this issue. We believe that more guidance is necessary to improve understanding and clearly state the what is expected of industry stakeholders.

Duke Energy would also like to highlight the topic of storage, and recommend that the drafting team consider discussing its importance relative to virtualization. Virtualization cannot be done without some type of storage. More guidance around this topic, and what should be considered by an entity when addressing this issue is needed.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Current CIP-005 does not describe how to handle these boundaries or if any additional protection / configuration is required. The current CIP-005 is based on physical connections and a physical inspection. This does not work well at all with virtual systems. If a virtual host spans multiple networks, the standards must address how to treat each component of the virtual system. There must be some framework for grouping of systems on a host such that guest systems of a different security level are not mixed with high security systems.	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Clarify security control requirements when CIP and non-CIP resources are in a shared environment.	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
See response 2 above. Logical technologies are becoming the standards at all layers of the OSI model except the physical and data link layers; virtual routers, switches and firewalls are commonly used tools. The specific criteria the SDT expects entities to abide by when it comes to partitioning the physical and logical layers of CIP and non-CIP protected assets is a line that needs to be clearly addressed.	
Likes 0	
Dislikes 0	
Response	

Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
To ensure consistency of implementation, modifications would help ensure that proper controls and architecture are implemented to reduce risk to BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
Answer	Yes
Document Name	
Comment	
From the CIP compliance standpoint, one of the reasons to isolate virtualized environments, whether physical or virtual, is to allow for different impact level for each environment. It is unclear at this time, the SDT's intent in allowing mixed mode configurations. As currently written, CIP-005-5 requires all components contained in a virtual system to be protected at the impact level of the highest single component of the system. CIP-005-5 would need to be revised to allow for mixed impact levels within a single virtual host. Concerning virtual networks, network devices can have multiple logical networks configured (e.g. virtual local area networks (VLANs)). Physical or virtual devices perform "logical isolation" when configured such that some network interfaces are available inside an ESP, and other interfaces are outside an ESP and the two networks cannot communicate with each other inside of the device. This would not prevent the VLANs configured inside the device from communicating through an EAP.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

NRG recommends that the standards need to allow for mixed trust devices as long you can logically separate them. The CIP standards need to be modified to support this because currently they do not address this. Not all companies have the resources to have multiple hypervisors for both CIP and Non-CIP. (The Hypervisor would need to be operated as the high water-mark).	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
From the CIP compliance standpoint, one of the reasons to isolate virtualized environments, whether physical or virtual, is to allow for different impact level for each environment. It is unclear at this time, the SDT's intent in allowing mixed mode configurations. As currently written, CIP-005-5 requires all components contained in a virtual system to be protected at the impact level of the highest single component of the system. CIP-005-5 would need to be revised to allow for mixed impact levels within a single virtual host. Concerning virtual networks, network devices can have multiple logical networks configured (e.g. virtual local area networks (VLANs)). Physical or virtual devices perform "logical isolation" when configured such that some network interfaces are available inside an ESP, and other interfaces are outside an ESP and the two networks cannot communicate with each other inside of the device.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
The standard must address new technologies which would allow security groups and other means of virtual separation within the virtualized environment. This includes virtual firewalls, switch instances, and other mechanisms which can be used to secure virtual hosts from each other.	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

Absolutely! In order to account for the sharing of physical virtualization infrastructure for NERC CIP and no-NERC CIP assets the requirements need to be updated to account for virtual LANs, Virtual Firewalls, and the protection of the base hypervisor and physical infrastructure. It is possible to manage this in a secure and auditable fashion but the current standards do not account for how to collect and verify the correct level of separation and security controls.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	Yes
Document Name	

Comment

Auditors have evolved over time significantly in what they consider mixed trust, making it hard for entities to be inline with a moving target. The standards should clearly define by a deterministic process or via specific examples what the limits are on sharing infrastructure between CIP and non-CIP systems. It may be better to prescribe security controls that must exist when sharing, rather than forbidding the sharing due to the existing of technologies which leverage shared technology while providing significant isolation.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

Seattle suggests that the concept of ESP needs to be made even more “logical” in nature, removing all vestige of a physical nature. To achieve this end, it might help to assign the revised concept a new name that does not implicitly imply anything physical (as does the term “perimeter”). Perhaps “electronic security isolation” or ESI?

Seattle further wishes to see virtualization concepts to expanded to address cloud-based systems. We are highly frustrated, for example, that NERC itself appears since early 2015 to have employed cloud storage for sensitive E-ISAC information including CIP incident reports from registered entities (see slide 6 of ES-ISAC Update in: http://www.nerc.com/gov/bot/botsotc/board%20of%20trustees%20%20standards%20oversight%20and%20tech1/sotc_presentations_february_2015.pdf*) and yet has been unable to provide audit guidance as to whether the cloud systems with the FedRAMP protections would satisfy the security requirements of CIP-004 and CIP-011. We encrouage the SDT to address cloud matters if possible.*

Likes 0

Dislikes 0

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	Yes
Document Name	

Comment

Absent any definitive requirement statements in CIP-005-5 about virtualization and the use of “mixed trust” configurations, Regional Entity auditors have, largely be default, become the arbiters in any dispute over whether or not a given “mixed trust” implementation is in compliance.

Likes 0

Dislikes 0

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

Parameters of an ESP within a virtual environment require clarification.

Likes 0

Dislikes 0

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CenterPoint Energy agrees with EEI's comments. If the intent of the SDT is to allow sharing of physical infrastructure between CIP and non-CIP Cyber Assets through virtualization, then language should be added addressing isolation methods.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP does feel this needs to be addressed in CIP-005-5; however, it is unclear what the modifications would look like at this time. More information is needed and the SDT should perform an evaluation of the impact these modifications will have on the standards. SRP also requests clarification regarding hypervisors. Would a hypervisor be considered a BES Cyber Asset?

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF

Answer	Yes
Document Name	

Comment

This should be clarified in the standards, since without explicit direction on this issue, it is left to the interpretation. The SDT should be mindful to provide these clarifications at the objective level in order to prevent becoming too prescriptive and to help future proof the standards.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Yes, in order for CIP and non-CIP environments to share a physical infrastructure via a virtualized environment, additional language in CIP-005 would be helpful to provide guidance for what methods are considered to be adequate to overcome risks and provide secure isolation or separation of the environments.

Having said that, Exelon does not currently envision undertaking the risk inherent in utilizing a “mixed” virtualized environment to host CIP and non-CIP VM’s, unless the entire “mixed” environment is afforded NERC CIP protections. In other words, we would not want to trust implementing security only at the software level to isolate virtualized CIP and non-CIP components.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	Yes
Document Name	

Comment

The ability for logical separation between BCSs and non-CIP Cyber Assets should be addressed. This includes the ability of a network switch to perform the logical separation as well as virtual environments.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

It is BPA’s position that CIP-005-5 would benefit from being modified to a security objective-oriented standard rather than a requirements-based standard. The security objective in this case would be isolation of CIP-applicable Cyber Assets from Cyber Assets that are out of scope of CIP controls.

The mechanisms of that protection are primarily Boundary Protection and Control of Network Ports, Protocols, and Services (SANS 20 Critical Security Controls).

CIP v5 narrowly focuses on routable protocols and Layer 3 controls and does not address the other layers of the OSI model. For example, under CIP-005-5 Layer 2 protocols are not addressed and can convey malware as well as allow information exfiltration and cyber-attacks even if no routable IP communications are present. Controls for these protocols should not be limited to or defined by Layer 3/4 ACLs on a firewall or router as the only or even the best means of achieving in-bound and out-bound access control. Entities need the opportunity to provide technical controls at whatever conceptual layer is appropriate to meet the security objective.

BPA recommends expanding CIP-005 language to include security zones with the ESP construct. When framed in terms of Boundary Protection, a security zone is more inclusive and granular because it is not limited to routable protocols at the OSI Model's Layer 3. A security zone construct does not force any particular interpretation or control onto serial or other non-routable means of transporting data or accessing the management plane of any systems. Security zones apply to physical and logical separation equally. An example of logical isolation provided by other than ACLs would be when a hypervisor provides isolation between Guest VMs or between Virtualized Network Functions. This isolation is implemented in the control plane by means of logic embedded in code base (NIST SP 800-125A – Draft, Section 1.2: Hypervisor Baseline Functions) and not at a conceptual network layer.

Current CIP standards take a broad stroke approach by requiring the protection of all cyber assets within an ESP in a singular manner at the highest impact level of controls. This is not cost effective or flexible enough for individual entities' needs. Security zones provide a scalable means of appropriately protecting Cyber Systems of differing security risks by further isolation within the zone.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	

Comment

The SDT should consider requiring additional controls for the Electronic Security Perimeter including the current access control lists in CIP-005-5, Part 1.3.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Wesley Maurer - Lower Colorado River Authority - 1,5,6

Answer

Document Name

Comment

Abstains from vote. LCRA seeks clarification on types of modifications SDT would implement prior to voting yes or no.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Modifications are not required to address the issue since, virtual environments should be treated the same as physical environments.

Such configurations can exist; the hypervisor (physical infrastructure) that is shared between BES Cyber Systems and other non-CIP Cyber Assets must be protected at the impact level of the BES Cyber System.

Furthermore, proper isolation (network segmentation, DMZ, virtual firewalls, vlans, etc,) must be implemented to reduce the risk of non-CIP Cyber Assets impacting BES Cyber Systems (e.g. Denial Of Service (DoS) attack).

Likes 0

Dislikes 0

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5,6

Answer

Document Name	
Comment	
LCRA Transmission Services Corporation (TSC) has chosen to abstain from vote. LCRA TSC seeks clarification on types of modifications SDT would implement prior to voting yes or no.	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	
Document Name	
Comment	
Abstains from vote. LCRA TSC seeks clarification on types of modifications SDT would implement prior to voting yes or no. Concerning virtual networks, network devices can have multiple logical networks configured (e.g. virtual local area networks (VLANs)). Physical or virtual devices perform “logical isolation” when configured such that some network interfaces are available inside an ESP, and other interfaces are outside an ESP and the two networks cannot communicate with each other inside of the device. This would not prevent the VLANs configured inside the device from communicating through an EAP.	
Likes 0	
Dislikes 0	
Response	

5. The SDT asserts that VLANs providing logical isolation are not addressed explicitly in CIP-005-5, and controls may be necessary to isolate BES Cyber Systems. Are the current requirements of CIP-005-5 sufficient to address logical isolation using VLANs? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
The current Electronic Security Perimeter definition establishes the protective enclave at a network (Layer 3). This is further identified in CIP-005-5, Part 1.3 access control lists. VLANs (layer 2) have not been an acceptable approach to establishing an Electronic Security Perimeter with a layer 2 switch; the switch cannot afford the required controls of Part 1.3. The SDT should clearly identify at what OSI model layer the SDT is asserting an Electronic Security Perimeter can be established and require controls to ensure isolation.	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes the same modifications necessary to make CIP-005-5 adequate to question 4 would apply to addressing the specific question of 802.1 Q VLANs providing adequate logical isolation in question 5. The security objective should be to provide isolation by means of Boundary Protection as well as Control of Network Ports, Protocols, and Services. Legacy software vulnerabilities that have long since been patched or known exploits that are mitigated through proper configuration should not require the blanket rejection of VLANs as a component of a particular entity’s specific security scheme. Newly discovered exploits and vulnerabilities are addressed through CIP-007 testing and patching, CIP-010 baseline configuration, change management, vulnerability scanning and assessment.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No

Document Name	
Comment	
Please reference the answer provided for #4.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
Exelon agrees that the current requirements of CIP-005-5 do not explicitly allow for VLANs providing logical isolation. Exelon has serious concerns that virtual isolation may not be adequately secure, and rewriting the CIP Standards is not the answer. There may not be an acceptable way to revise CIP standards to allow use of VLANs for mixed environments, as the risk for compromise is too high. Virtualization is one configuration mishap away from revoking logical isolations, no matter how well thought out, should the management layer collapse into a single unified network. Employing technology that eliminates the possibility of collapse provides a much more effective mitigation by removing the possibility of any collapse. Firewalls provide an active control environment meeting CIP-005-5 by utilizing a comprehensive security toolset, including rulesets, the deny-all rule, bidirectional controls, scanning for malware, etc. However, a Layer 3 network switch does not have these features, and cannot provide the same level of security. Exelon contends that implementing VLANs using a Layer 3 network switch will not meet current requirements or security needs. While VLANs can be configured to go thru a firewall, the switch itself is still vulnerable to reconfiguration to directly connect separated VLANs. Layers of manual processes to manage the risks are the only alternative, and would be considered weak security as well as additional cost (possibly offsetting any cost-savings from virtualizing). As such, we consider that VLANs are not an appropriate technology to provide adequate security in a CIP environment.	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	No
Document Name	
Comment	
This should be clarified in the standards, since without explicit direction on this issue, it is left to the interpretation of auditors. PJM suggests that it should be clarified at the objective level and should not be prescriptive, to account for different implementation methods.	

Likes 0	
Dislikes 0	

Response

Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

While traditional network technologies such as VLANs can provide an an easy way to isolate traffic within a network, software-defined networking technology provides a much stronger protection by not forwarding tagged packets in the first place. I assert that methods of isolation are not explicitly addressed within CIP-005-5 and that expanded language should be added to detail additional controls. I also assert that if language such as “physical separation” is used that controls such as software defined networking be recognized as “physical separation.” If a software defined networking Ethernet switch does not have any flow rules programmed into the switch, then there is no physical connectivity (deny by default) with devices attatched to the same switch. Software-defined networking employs a superior approach in that no additional data must be inserted into the header (e.g., VLAN TAG), rather the grouping can be accomplished with flow rules and executed at the packet forwarding devices (SDN Switches) in a highly simplified and automated manner. This ensures the tamper resistant flow of communication, limiting what an adversary could do with a man-in-the-middle attack, e.g., modifying the VLAN tag.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP does not feel this is addressed in any of the CIP-005-5 requirements. CIP-005-5 addresses ESPs, which are a layer 3 concept. VLANs are a layer 2 concept. Addressing this in CIP-005-5 would assist with clarifying acceptable isolation. SRP requests clarification regarding why VLANs are a concern. Is using VLANs for isolation a concern because of inadvertent traffic between VLANs (i.e., VLAN hopping)?

What about the shared storage from which the hypervisor serves VMs? Is the entire storage array CIP if there is a single CIP VM on it?

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy believes VLANs are a separate topic from "virtualization" as it relates to virtual machines and that the requirements around VMs will be difficult to apply equally to network infrastructure. These requirements, when written, should be separate without an attempt to write one requirement applicable to all virtual technology.

CenterPoint Energy believes the logical protection afforded by a VLAN is well established, having been in broad usage in industry for decades, but has risks not addressed in existing requirements. Entities should be free to maximize hardware utilization through use of VLANs if they choose. The practical examples of VLAN-escape attacks, exploiting default VLANs or the trunk protocol used to manage VLANs, are well known and easily mitigated with switch configuration. The requirements of CIP-005 do not address these mitigations, and the Cyber Vulnerability Assessment may or may not address them. To adopt VLANs securely, CenterPoint Energy recommends creating a new CIP-005 requirement and suggests the following wording: "Implement a process to ensure that a virtual network infrastructure, fully or partially within an Electronic Security Perimeter, is configured to mitigate the risk of VLAN escape attacks."

Furthermore, the terms "connected using a routable protocol within or on an ESP" in the Protected Cyber Asset definition is confusing in relation to virtual machines. CenterPoint Energy recommends clarification to the PCA definition:

1. A hypervisor hosting a BCS virtual machine must be a BCS since it can impact the availability of a BCS within 15 minutes.

2. An asset hosted by a hypervisor in an ESP that is not part of the BCS within the same ESP must be treated as a Protected Cyber Asset.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

CIP 005 does not sufficiently address modern network topologies. The use of layer-2 VLANs should be an explicitly acceptable method of segregation for BES Cyber Systems and non-CIP Cyber Assets on a shared physical network infrastructure.

Security measures to protect virtualized workloads can be implemented in an equivalent security posture as a traditional physical workload. Complete datapath isolation can be achieved on routers and firewalls using virtualized routing tables and virtualized operating systems. This virtualized datapath isolation provides a secure foundation for enabling workloads, such as virtual BES Cyber Systems and non-CIP Cyber Assets, to share physical network infrastructure.

Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST agrees with the SDT's view that CIP-005-5 does not address VLANs and how they might be logically segregated. Needless to say, this lack of information is making it difficult for entities to determine whether or not a given VLAN implementation will satisfy Regional Entity auditors.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
The SDT has made good progress in their white paper identifying many of the concepts and approaches necessary for virtualization, and we support continued development along these lines. We are concerned, however, about relying too heavily on a single model of virtualization to frame the concepts and approaches for new requirements, and urge the SDT to consider more broadly the various implementations and possibilities of virtualized systems in addition to the reference model they have created.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	

If the SDT asserts that VLANs isolation is not sufficient security to protect the ESP from communication beyond the ESP, explicit language forbidding the practice is necessary which would open a can of worms since there will always be emerging security issues too numerous to itemize in regulations. When entities do not use a best-practice, or common-practice approach to security, it is probably not best addressed in CIP regulations, but rather as an evidence-based, educational communique indicating the risk of a certain approach. Any entity that continues to take on such a risk can be later evaluated on their CVA process as to why they are not remediating risks above a certain level.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
The requirements need to be enhanced to specify the expectations for using VLANs within an EAP. VLANs are used extensively now to perform the level of logical exception but these are almost exclusively done at the port level.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	No
Document Name	
Comment	
The standard needs to be revised to take technologies that have been around for a very long time. Such as VLAN tagging and separations and 802.1Q trunking. The standard should say when an 802.1Q trunk consists of VLANs that are both outside the ESP and inside the ESP that the layer 3 route must terminated at an EAP.	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No

Document Name

Comment

The SDT should add requirements to address all the risk presented in the virtualization risk map file.

The SDT has identified certain risks inherent to virtualization regarding the use of centralized management automation. The SDT is proposing to classify *Centralized Management System* (CMS) explicitly as a type of applicable system for some CIP requirements. In examining management architecture and risk management for virtual environments, the SDT identified an increased risk inherent to the span of control of hypervisor management consoles. Further, the SDT noted that similar risks exist in CMSs used to manage physical devices, and recognized these risks may not be fully addressed in current CIP standards and the *EACMS* definition. The SDT is considering a new definition of this class of system.

The proposed *Centralized Management System* (CMS) definition is:

A centralized system for administration or configuration of BES Cyber Systems, including but not limited to systems management, network management, storage management, or patch management.

Likes 0

Dislikes 0

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG recommends that the current CIP-005-5 standards do not sufficiently address the logical isolation and separation using VLANs. If entities could be allowed to do this, it would be beneficial to them and to the auditors. VLAN’s can be separated and standards can be applied to allow this separation.

Likes 0

Dislikes 0

Response

Scott Downey - Peak Reliability - 1

Answer	No
Document Name	

Comment

VLAN isolation is one of the oldest methods of securing networked systems, particularly when VLANs are then trunked through firewalls for VLAN-to-VLAN management. The SDT hasn't addressed this level of virtualization in an environment.

Likes 0	
Dislikes 0	

Response

Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC

Answer	No
Document Name	

Comment

Clarify security control requirements when CIP and non-CIP resources are in a shared environment.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Current CIP-005 program does not address VLAN at all and it is very difficult to determine what the SDT / NERC requires. There is no framework or guidance on network architecture. The standard does not address where physical separation is required, and where the use of VLAN or other virtual network technology is appropriate or beneficial. The CIP-005 standard does not address communication requirements between systems, or give guidance on separating systems with external communication.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy believes that the current requirements in CIP-005-5 do not adequately address logical isolation using VLANs. More guidance on this issue would be beneficial to to improve understanding and clearly state the what is expected of industry stakeholders.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	

Comment
The SDT should consider defining a Virtual Security Perimeter (VSP) or modifying the existing ESP term in a way that would apply to cyber assets associated with a hypervisor and dependent virtual machine relationship to address needed controls in such a situation. Suggest that the SDT provide guidance on the use of the isolation of traffic provided by VLANS as an electronic control.

Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	No
Document Name	

Comment
Entergy agrees with the concept of logical isolation as described above, but has received contrary guidance related to this concept from outside entities. Entergy does not agree that additional controls are required for logical isolation. However, providing clarity on the applicability of existing CIP-005 controls related to logical isolations would benefit all parties. The SDT has identified certain risks inherent to virtualization regarding the use of centralized management automation. The SDT is proposing to classify *Centralized Management System* (CMS) explicitly as a type of applicable system for some CIP requirements. In examining management architecture and risk management for virtual environments, the SDT identified an increased risk inherent to the span of control of hypervisor management consoles. Further, the SDT noted that similar risks exist in CMSs used to manage physical devices, and recognized these risks may not be fully addressed in current CIP standards and the *EACMS* definition. The SDT is considering a new definition of this class of system.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

There is no construct provided to apply layer 2 controls to technologies like VLANs. Adding this construct could allow for future proofing of the use of isolation technology such as VLANs, VXLANs, MPLS, etc.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

The SDT should consider defining a term such as “Virtual Security Perimeter (VSP)” or modifying the existing ESP term to allow for the isolation fo BES Cyber Assets or BES Cyber Systems using virtual technologies.

While CIP-005 is applicable to High and Medium Impact only, therefore, request the SDT to address VLANs for Low Impact in CIP-003. Currently, a VLAN may be part of the electronic security controls (per CIP-003-6 and CIP-003-7) for a low impact BES Cyber System. The determination by the SDT to allow or eliminate these VLANS in CIP-005 may have an unintended corresponding consequences on the interpretation of CIP-003 for low impact.

Suggest that the SDT provide guidance on the use of the isolation of traffic provided by VLANS as an electronic control.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	No
Document Name	

Comment

Southern Company does not agree with the SDT assertion that VLANs providing logical isolation are not addressed in CIP-005-5. The CIP-005 Standard requirements can be applied to VLANs without additional clarification as CIP-005 requires that applicable Cyber Assets must

reside in a "logical border" and any external routable connectivity through that logical border must be through an identified Electronic Access Point, and that EAP must deny all traffic except for what is explicitly allowed. These objectives can be met with physical or virtual networks and logical isolation.	
Likes 0	
Dislikes 0	
Response	
Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	
CIP-005 language changes should not be limited to VLANs. It should also apply to virtualized routing instances, firewall contexts, and virtual network appliances. You can still control the boundary using virtual mechanisms if you explicitly allow VLANs it implicitly disallows other virtual solutions. You should use more general terms and not use VLANs as the sole mechanism.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
No the current standard doesn't address VLANs or the concepts at all. The requirements, applicability and measures would all have to be modified.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation recommends defining and adding VLANs, Hypervisor, Virtual Machines, Virtual Networks and Virtal Storage to the NERC Glossary of Terms and identifying which VLAN features are to be included in CIP-005-5.

Likes 0	
Dislikes 0	

Response
David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

VLAN implementation is all ready being used and relied on extensively in CIP environments. CIP-003-7 Model 9 also supports use of virtualization, so it seems VLANs have already been adopted as acceptable.

What is not clear is that CIP-005 does not state that CIP related and non-CIP related though isolated on VLANs can be mixed on a single physical switch. Up to this point we have used seperate switches for CIP related traffic and VLANS have been only used to further subdivide the CIP related traffic. For instance into a SCADA network and a DMZ supporting EACMS and PACS. An explicit statement allowing mixed virtually isolated CIP and non-CIP traffic on shared physical host networking devices, and under what conditions, if any, would give more compliance certainty about VLAN acceptibility in these circumstances.

Also, as a second concern, it might be pruduent to disscuss the issue that it is inherently easier to misconfigure virtual networking and VLANS in such a way that a setup is intended and thought to be secure and compliant with CIP-005 but in fact is not, even though it appears to be "working". Mandating an independent review/verification by a second person/party (fresh set of eyes) or actual security testing during comissioniong or some other verification measure might be an appropriate mitigation for this risk in a virtual environment.

Likes 0	
Dislikes 0	

Response
Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC agrees that the regulation is not clear as to when layer 2 or layer 3 VLANs constitute access, or the requirement for an EAP on the device configured to use VLANs. Additionally, ATC supports EEI’s comments in that CIP-005-5 is insufficient because it does not enable the use of VLANs for logical isolation since the requirements cannot be met and the use of VLANs (i.e., layer 3 switch) to logically isolate CIP from non-CIP environments does not provide the same level of security as a layer 2 switch with a firewall.

Likes 0	

Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
If the host (or hypervisor) carries routable protocol communications destined for both inside and outside of the ESP, then it would itself be a conundrum (it should be a BCA or PCA if inside, but cannot be a BCA or PCA if outside). The current language in CIP-005-5 (and CIP-002, CIP-007, and CIP-010) do not support this current configuration and would need to be modified to allow it.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
There is no clear standard requirement language at present that excludes the usage of VLANs, and it is not clear through inference as to under what conditions VLANs can be used. Recommend the standard requirements provide clear distinctions regarding VLAN usage and requirements for such configurations.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

AZPS respectfully submits that VLANs have the ability for appropriate controls, but that, previously, there has been inconsistency about whether VLAN controls are adequate to meet the current ESP-related requirements. AZPS encourages the SDT to review and revise CIP-005-5 such that VLANs and their applied security controls can be utilized as an ESP boundary.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
As implemented, AEP believes VLAN configurations provide sufficient records of and controls for logical network segmentation. And, there is no need for a requirement to dictate a standard of proof.	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

The current requirements of CIP-005-5 are clear in their assertion that virtualized systems may reside within an ESP. ESPs should be isolated from other networks. Virtualized systems should not cross ESP boundaries. We do not believe that logical controls are sufficient to define an ESP boundary. VLANs should not be permitted to define ESP boundaries.

We are concerned that the SDT is confusing VLANs and hypervisor based virtual switches.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	Yes
Document Name	

Comment

More clarification is needed for the question.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE

Answer	Yes
Document Name	

Comment

The current requirements of CIP-005-5 are clear in their assertion that virtualized systems may reside within an ESP. ESPs should be isolated from other networks. Virtualized systems should not cross ESP boundaries. We do not believe that logical controls are sufficient to define an ESP boundary. VLANs should not be permitted to define ESP boundaries.

The proposed *Centralized Management System* (CMS) definition is:

A centralized system for administration or configuration of BES Cyber Systems, including but not limited to systems management, network management, storage management, or patch management.

The SDT should add requiremnts to address all the risk presented in the virtualization risk map file.

Likes 0	
Dislikes 0	

Response

Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
The current requirements related to EAPs and inbound and outbound access controls are sufficient. However, guidance would help in showing that the use of VLANs is an adequate means of logical isoloation and physical isolation on dedicated equipment is not required.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Logical isolation is not the equivalent of security isolation. While VLANs are useful within environments containing different levels of trust to reduce broadcast domains and to isolate different types of traffic, VLANs should not be considered a security mechanism used to separate highly critical traffic from untrusted traffic. As traffic not within CIP scope must be considered as completely untrusted by the CIP audit teams, mixing non-CIP-scope traffic and CIP traffic within the same physical network should not be considered acceptable.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
The current requirements related to EAPs and inbound and outbound access controls are sufficient. However, guidance would help in showing that the use of VLANs is an adequate means of logical isoloation. Physical isolation on dedicated equipment is not required.	
Likes 0	

Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Addressing the routable subnets in CIP005 inherently addresses the VLANs at layer 2.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Kansas City Power and Light supports Edison Electric Institute’s Comments.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
The current requirements related to EAPs and inbound/outbound access controls suffice. However, guidance would help show the use of VLANs is an adequate means of logical isolation and physical isolation on dedicated equipment is not required.	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	
Document Name	
Comment	

Abstains from vote. LCRA TSC seeks clarification on types of modifications SDT would implement prior to voting yes or no.

The SDT has identified certain risks inherent to virtualization regarding the use of centralized management automation. The SDT is proposing to classify *Centralized Management System* (CMS) explicitly as a type of applicable system for some CIP requirements. In examining management architecture and risk management for virtual environments, the SDT identified an increased risk inherent to the span of control of hypervisor management consoles. Further, the SDT noted that similar risks exist in CMSs used to manage physical devices, and recognized these risks may not be fully addressed in current CIP standards and the *EACMS* definition. The SDT is considering a new definition of this class of system.

The proposed *Centralized Management System* (CMS) definition is:

A centralized system for administration or configuration of BES Cyber Systems, including but not limited to systems management, network management, storage management, or patch management.

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	
Document Name	
Comment	

LCRA TSC has chosen to abstain from vote. LCRA TSC seeks clarification on types of modifications SDT would implement prior to voting yes or no.

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Yes, the current requirements of CIP-005-5 are sufficient to address logical isolation using VLANs, physical or virtual networks.

VLANs can meet the definition of an ESP, which is “*the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol*.”	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	
Document Name	
Comment	
Abstains from vote. LCRA seeks clarification on types of modifications SDT would implement prior to voting yes or no.	
Likes 0	
Dislikes 0	
Response	

6. Do you agree with the proposed definition of CMS? If not, please provide alternative language for the definition and your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS respectfully submits that the development and creation of additional terms and asset classifications is unnecessary.   As discussed above, all cyber assets (physical or virtual) can be classified in existing classification of Cyber Asset if it is modified as recommended in AZPS's response to Question #2. Hence, AZPS does not agree with or support the creation of a new definition for CMS or the use of such a term in the CIP Reliability Standards.

Likes 0	
Dislikes 0	

Response

Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

This new definition seems broad and is hard to support without a clear idea of how it will be used in requirements and how this will impact existing CIP implementations. The scope of the new requirements also needs to be very clear.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro

Answer	No
Document Name	

Comment

The proposed definition is too general and appears to potentially include compliance management systems that are relational databases used to manage compliance activities pertaining to BES Cyber Systems. This comment is in reference to the usage of 'centralized system for administration', and the additional language of 'including but not limited to….'. Recommend adding further qualifiers to the definition that explicitly mention virtualization applications of said systems or systems used to manage physical devices, which leaves compliance management systems that are not used in such context, out of scope.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

No.

KCP&L identifies several points of concern and offers an alternative. The alternative, in concept, is not perfect; we offer it to address our concerns and the inherent risks identified by the SDT.

Concerns

1. **Impact to Applicability of Existing CIP Standards**: A new CMS definition is considerable and far-reaching; it requires a review of applicability in the complete suite of CIP Standards and, where impactful changes are identified, the effected Standard going through the revision process.

2. **Impact on Entities**: A new CMS definition requires entities to review and incorporate the new definition and subsequent revisions to Standards because of the new definition into their documentation, policies and procedures.

3. **Potential Scope Expansion**: The proposed CMS definition's scope may potentially swell to include physical systems.

Alternative

The concept is to move away from a CMS new asset type approach to incorporating management devices into existing EACMS asset types. To integrate this concept into the existing NERC EACMS Glossary definition, we offer:

Electronic Access Control, Monitoring or Management Systems (EACMS):

Cyber Assets that perform electronic:

1. Access control of the Electronic Security Perimeter(s) or BES Cyber Systems;

2. Security incident and event monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems; and,

3. System management functions associated with the Electronic Security Perimeter(s) or BES Cyber Systems.

EACMS include, but are not limited to, Intermediate Systems; firewall management; patching management; virtual system management; access control; security incident and event monitoring; and server and workstation management. Management systems are limited to systems capable of modifying the configuration; applying patches, updates or code changes; remotely starting, shutting down, or restarting the asset—rebooting, its services or processes; or has the capability of altering a Cyber Asset's function within in a BES Cyber System.

In addition to the revised EACMS glossary term, a revision to CIP-007-6, Table R1, adding a new subpart under the R1 Table could address when there are instances Out-of-band networks required for Cyber Asset management. The new subpart to Table R1, Ports and Services, would apply to High

Impact and Medium Impact EACMS used for management devices to connect to things like iLOs, virtual switches, firewalls, network devices, and devices that require a port on a network that is separated physically or logically from normal production traffic.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
In practice, how does the definition of a CMS differ from that of an EACMS? How would the risks be mitigated differently? Without any clear intent of how the SDT plans to implement a new defition, PacifiCorp cannot support the creation of one.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Additional clarity is needed to understand how this new term will be applied in the CIP requirements and how this term will impact existing CIP implementations.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

This new definition seems broad and is hard to support without a clear idea of how it will be used in requirements and how this will impact existing CIP implementations. The scope of the new requirements needs to be very clear. For example, is this term intended to apply only to virtualized environments or will it extend to other management systems? Will this create duplicative classifications, e.g., as an EAMCS and a CMS or as a PCA and a CMS? Also, CMS is an acronym commonly used for Content Management Systems, which may cause confusion.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	No
Document Name	
Comment	
LCRA seeks language specifying that only devices which make configuration changes would be in scope. Network monitoring software can be part of a network management system but if the network monitor does not make configuration changes it should not be considered a Centralized Management System.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
In the standard the Intermediate System definition exists, and could be leveraged to meet this objective. Additionally, if a separate definition were to be created, while it refers to BES Cyber Systems, the scope expands as a function of the applicable systems and associated Cyber Assets within the parts of the standard (unintended consequences) Additionally, ATC supports EEI's comments that this new definition seems broad and is hard to support without a clear idea of how it will be used in requirements and how this will impact existing CIP implementations The scope of the new requirements needs to be very clear. For example, is this term intended to apply only to virtualized environments or will it extend to other management systems? Will this create duplicative classifications, e.g., as an EAMCS and a CMS or as a PCA and a CMS? Also, CMS is an acronym commonly used for Content Management Systems, which may cause confusion.	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
A reservation regarding the proposed definition is that it does not define a threshold for when a supporting cyber asset becomes a CMS. Is it if it supports a single BCA? Or multiple? Inclusive or exclusive of PCAs, EACMS, PACS? Does it apply if only a single BCS is managed? Or more than one?	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends providing clarification on the proposed definition of CMS. Does the SDT intend for the proposed definition of CMS apply to CIP-010-2?	
Likes 0	
Dislikes 0	
Response	
Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	
We do not think you should differentiate CMS from EACMS. If anything, you should broaden the definition of an EACMS to include other central management and administration systems. Many of these systems perform both functions, which would only increase ambiguity.	
Likes 0	
Dislikes 0	
Response	

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
In the absence of more information on how it would be used, Southern Company does not agree with the proposed definition of Centralized Management System (CMS). Assuming the typical virtualization environment, management consoles may be within the ESP and protected at least as PCA's, including CIP-010 change management for the console and all configured BES Cyber Systems. Alternatively, management consoles classified as an EACMS may be used to support many EACMS outside an ESP, and therefore would complicate the identification, classification, and applicable requirements of various Centralized Management Systems used in different capacities (BCS, EACMS, PCA).	
Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
CMS's that meet the definition of a BES Cyber Asset would already be identified in the CIP-002 assessment process since they would be Cyber Assets that, if misused, could have a 15 minute impact on the BES. This was not an issue that was identified by FERC. A revisions to the CIP standards caused by this expansion of scope could cause additional delays in the current implementation thereby delaying the security that the standards are meant to insure. We suggest that this term not be included as part of this CIP modification project. If the SDT determines that there is an additional risk associated with the CMS for hypervisor management consoles, this risk should be addressed without pulling in unrelated systems.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	

PSEG supports Edison Electric Institute’s comments.

Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The definition is well crafted, but the term “centralized” may contain some ambiguity in this context. Must the CMS be centralized in one device? In one location? For one function? Suggested revision:

Centralized Management System (CMS): A system for administration or configuration of multiple BES Cyber Assets, including but not limited to systems management, network management, storage management, or patch management.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not agree with the proposed definition of Centralized Management System. As written, the definition is too broad, and could possibly bring in devices not intended by the SDT (i.e. Corporate laptops). The examples identified appear to be appropriate, but the capability aspect alluded to in the definition makes this definition too broad in scope.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

A CMS should be managed/protected. The definition does not give clear criteria on what is included as a CMS. How is the term “administration” defined and what type of administration is included. If a system provides operational monitoring but cannot change an end point is it included? If a system stores backup configuration files or data is it included? How is the term “configuration” defined? The text in the statement “including but not limited to” should be moved to a guidance section and do not belong in a definition. There is no clear definition of what functions a “systems management system” performs.

The types of devices in the examples typically require Interactive Access to Cyber Assets, and as such are already in scope of the standard based on CIP-005 R2. A network communication centric identification is better suited to these types of assets.

Also, it’s not clear how to differentiate a CMS from an EACMS. For example, an Active Directory server seems to fit the definitions of both CMS and EACMS. Should it be designated as both, and if not, which designation should take precedence?

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	No
Document Name	

Comment

The term "CMS" in this instance is too generic. It would be beneficial to include the specific forms of systems management the SDT intends to include in the standard (patch management, application deployment, virtualiztion management, storage management, and so on), and further, the individual included components of a management system should have requirements tailored to the specific function (see response 7 below).

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE

Answer	No
Document Name	

Comment

Centralized management systems that meet the definition of a BES Cyber Asset would already be identified in the CIP-002 assessment process since they would be Cyber Assets that, if misused, could have a 15-minute impact on the BES.

Defining a new term and including it in the applicability columns of the CIP standards may add additional Cyber Assets to the existing CIP scope. This was not an issue that was identified by FERC. The revisions to the CIP standards caused by this expansion of scope could cause additional delays in the current implementation thereby delaying the security that the standards are meant to insure. We suggest that this term not be included as part of this CIP modification project

If the SDT determines that there is an additional risk associated with the CMS for hypervisor management consoles, this risk should be addressed without pulling in unrelated systems.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG has concerns that the proposed definition is too broad and includes systems that are beyond the virtual Hypervisor issue.

Likes 0	
Dislikes 0	

Response

Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6

Answer	No
Document Name	

Comment

The definition is too broad as written, making its intent unclear. If the intent of CMS is to cover hypervisor type technologies the definition should include the word virtual or other reference to management of virtual architecture.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Centralized management systems that meet the definition of a BES Cyber Asset would already be identified in the CIP-002 assessment process since they would be Cyber Assets that, if misused, could have a 15-minute impact on the BES.

Defining a new term and including it in the applicability columns of the CIP standards may add additional Cyber Assets to the existing CIP scope. This was not an issue that was identified by FERC. The revisions to the CIP standards caused by this expansion of scope could cause additional delays in the current implementation thereby delaying the security that the standards are meant to insure. We suggest that this term not be included as part of this CIP modification project

If the SDT determines that there is an additional risk associated with the CMS for hypervisor management consoles, this risk should be addressed without pulling in unrelated systems.

Likes 0

Dislikes 0

Response

Aaron Austin - AEP - 3,5

Answer No

Document Name

Comment

AEP does not support the definition as proposed and is not certain that it is appropriate without indication of the requirements the SDT believes such a definition would be applicable. The definition should be exclusive of Cyber Assets included in the scope of the EACMS definition. Without this exclusivity, entities will be forced to account for all possible combinations of cyber system types.

Likes 0

Dislikes 0

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5,6

Answer No

Document Name

Comment

LCRA TSC seeks additional clarification as to what devices are or are not considered CMSs.

Likes 0

Dislikes 0

Response

Michael Shaw - Lower Colorado River Authority - 1,5,6

Answer	No
Document Name	

Comment

LCRA TSC seeks additional clarification as to what devices are or are not considered CMSs.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

See comments for Question 7, below.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

It is possible to have virturalized CIP infrastructure that is not part of a BES Cyber system and would still need protections. Examples include EACMS infrastructure and intermediate systems. The SDT should consider the risks posed by vitualized EACMS devices in the CMS definition.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not agree with the CMS definition and the intent to add CIP requirements to the proposed asset category. First, the proposed CMS definition contains open ended wording subject to broad interpretation by auditors beyond the intent of the SDT. The proposed definition will expand the scope of CIP applicable systems. CenterPoint Energy believes the term should address the intended system explicitly in order to limit scope creep.

Centralized management systems could be in place to provide services to multiple systems within a data center, or enterprise-wide, both in and out of scope for NERC CIP. The required regulatory response of entities to comply with requirements to protect CMS, as yet unwritten, may be much broader than the intent of the SDT. In particular, the addition of patch management systems is a concern. If the CIP Standards dictate how entities deploy patches and restrict the ways this can occur, better solutions will be abandoned in exchange for compliant ones. This has already occurred in response to the malware signature deployment testing requirement. Patch management systems have no place in the CMS definition. Similarly, storage management is a huge area, often managed enterprise-wide. SDT is well advised to focus on protection of data per CIP-011 in storage rather than expanding scope of CIP to cover storage systems as well.

Finally, hypervisors are not listed among the examples even though this term is clearly meant to cover them.

As an aside, the acronym CMS is well-known and used in data centers to refer to a Content Management System and the new acronym might cause confusion.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Patch management is an act, not a system, and should not be included in the definition. Using the term “management” (systems management, network management, etc.) is much too broad, as it pulls in aspects of management that have no impact on the reliability of the BES. More emphasis should be placed on configuration. There should also be more definition around “administration.” SRP proposes revising the definition to, “A tool used for the configuration, turn-up, or deployment of BES Cyber Systems…”

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF

Answer	No

Document Name

Comment

PJM suggests adjusting the language to align with the structure of the approved EACMS and PACS definitions:

Cyber Assets that perform administration or configuration of BES Cyber Systems., including systems management, network management, storage management, or *patch management.*

Likes 0

Dislikes 0

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

Exelon is concerned with the proposed definition extending what “Centralized Management Systems” would be in scope for the CIP standards. A definition should focus on virtualization so as not to create confusion since not all centralized management systems are virtualized, and not all virtualized systems are for central management. Exelon understands that the CIP SDT has to refrain from using any specific terms that could identify any one vendor product.

One approach the CIP SDT could take, if they believe that there needs to be a definition for the management system, is to use “Virtualization Management System” instead of “Centraized Management System” along with the definition in this posting. This would correctly scope the applicability to not include other “Centrlized Management Systems.”

Likes 0

Dislikes 0

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
In examining virtualization, the SDT considered centralized management systems or consoles for these environments. These systems allow for the mass addition, deletion and modification of virtual machines and networks. Access to the control surface of a cyber system is known as the *management plane*. The management plane is where the virtual infrastructure is configured and managed by a limited group of administrators as opposed to the *data plane*. The data plane is where the end user’s access to the virtual machine’s business function takes place. To meet the security objective of protecting a BES Cyber System from threats in the data plane, the management plane should be isolated from the data plane. These types of controls are referred to as *out of band* management.	
Likes 0	
Dislikes 0	
Response	
Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Not addressed in v5. Industry must have some guidance as to what is defined and in scope.	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Centralized Management Systems are a huge issue for NIPSCO OT. We have wrapped a number of our CMS' into EACMS which causes a ton of grief for our operability. These suites of systems require special protections but not the same level as an EACMS. I agree with this definition as it identifies areas that are of significant security concern while potentially minimizing impacts to our operability. NIPSCO OT has taken a conservative approach with our management consoles and made all of them EACMS systems. This causes significant costs and difficult operability for my teams. I would encourage further development on this term and encourage that the requirements are placed somewhere between a TCA and an EACMS.	

Likes 0

Dislikes 0

Response

David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	Yes
Document Name	

Comment

There has long been uncertainty on how to address these types of assets. Please consider a new name of the term since this acronym is already overly used in different contexts. Please clarify that system health and statistic monitoring is not to be included within this definition.

Likes 0

Dislikes 0

Response

Lee Maurer - Oncor Electric Delivery - 1

Answer	Yes
Document Name	

Comment

There has long been uncertainty on how to address these types of assets. Also, please consider a new name of the term since this acronym is already overly used. Please clarify that system health and statistic monitoring is not to be included in this definition.

Likes 0

Dislikes 0

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

We support the general concept and approach, but are concerned that the concept, being new and unfamiliar to industry and auditors alike, may end up bringing other, non-CIP systems into scope or otherwise impact non-virtualized BES Cyber Systems. To minimize the risk of unintended consequences, *we suggest that the scope of a CMS be narrowed to apply only to virtual systems at this time. The expansion of the CMS concept to address risks that may be present in managing physical devices is beyond the SAR of this project.*

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

It is BPA's opinion that the SDT's proposed definition of CMS captures most types of systems that support automation with a large span of control and privileged access. A similar span of control risk exists in that EACMS is a type of CMS for electronic access but the term *EACMS* is specific to NERC CIP and used nowhere else in IT Security or Information Assurance in any other industry. This inherently limits the amount of expertise, guidance, and documentation available for solving the root problem of controlling access to CIP-applicable systems.

BPA recommends that the SDT should retire the NERC CIP defined term *Electronic Access Control & Monitoring System* from the NERC Glossary and adopt the industry solution *Authentication, Authorization, and Accounting* System (AAA System). Non-standard jargon should be avoided when adequate terms and concepts exist already. See link: http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-35/101-aaa-part1.html

Further, BPA recommends that the SDT should clarify in Guidelines and Technical Basis, that:

- AAA *clients* that subscribe to AAA services (e.g. via a protocol such as LDAP, RADIUS or TACACS+) but do not maintain any account information are not AAA Systems in themselves
- Remote access *clients* or terminal emulators that are used to connect to a CMS, are not a CMS in themselves

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	
Rather than introduce a new term, Texas RE recommends the SDT consider adjusting the existing EACMS definition, which has been applied (applicable systems) to the CIP Requirements already. Texas RE inquires which parts of the requirements would include the new definition of CMS?	
Likes 0	
Dislikes 0	
Response	

7. Do you agree with the SDT’s approach to reference the CMS specifically as a type of applicable system in the CIP standards? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
See comments to Question (6)	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST recognizes there are legitimate security concerns associated with systems used to manage and/or configure BES Cyber Systems and associated EACMS and PACS systems (especially, and for example, network firewalls whose interfaces include one or more EAP). However, N&ST is concerned that the SDT’s well-intentioned attempt to define “Centralized Management System” could result in significant pushback from industry and endless arguments about what type of system would meet the proposed definition of “CMS.” What does “centralized” mean? It is technically feasible (to borrow a phrase) for a firewall administrator to modify the configuration of multiple firewalls using his or her smartphone. Would doing so render his or her smartphone a CMS? N&ST believes that hypervisors used to create, modify, or remove virtual machines that qualify as BES Cyber Assets should themselves be evaluated as potential BES Cyber Assets or other Cyber Assets subject to CIP requirements, and that the Standards should make this clear. However, N&ST believes that security for other types of devices used for management and configuration in CIP environments is adequately addressed by existing requirements (e.g. CIP-005 requirements for Remote Interactive Access). This opinion is based, in part, on the fact many N&ST clients have chosen to locate systems used for the administration and/or configuration of BES Cyber Systems INSIDE defined ESPs, which makes them Protected Cyber Assets and therefore already subject to many CIP requirements.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No

Document Name	
Comment	
It is too soon to tell. The concept is fetching but we would want to see more details.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
There are so many ways once in the ESP to negatively affect BES systems. Single out CMS for addition scrutiny seems unnecessarily as all other CIP controls already apply. Potentially for devices that can effect multiple systems simultaneous, more attention could be called for in the area of recovery plans.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
The SDT should consider reviewing, revising, or replacing existing definitions of supporting cyber system types to achieve its goal of protecting those centralized cyber systems used to manage BCS or other related cyber systems.	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	No

Document Name	
Comment	
We do not think this is necessary if virtualized systems managing BES Cyber Systems are required to stay within the boundaries of an ESP.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
Answer	No
Document Name	
Comment	
The proposed definition of CMS is more general than just those types of CMS associated with command and control of virtual resource environments. This takes the discussion beyond the scope intended for addressing virtualization technology in the context of CIP. If the SDT decides to include CMS applicability, the definition should be refined to include only virtualization or addressed in a new CIP standards modification project. This type of systems are not addressed in the standard and represent risks that need to be addressed.	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	No
Document Name	
Comment	
There are a myriad of ways to manage systems. Trying to add these definitions now, and bringing those systems into the scope of the CIP standards, would be burdensome on entities, and provide very little risk management. For example, patch management systems frequently have methodologies to ensure that the content of the patch management system has not been tampered with (checksum, digital signatures, and so on). Further, entities very well may rely on logical separation of the management of systems from the user access of systems. Trying to create standards around these types of assets would create confusion and complexity, and not inherently improve security. There would also be overlap with existing definitions in the standards, such as EACM, which could also qualify as a CMS. Instead, focus on which types of management systems should be specifically included in the scope of the standards, and write requirements specific to those assets to ensure the integrity of the CMS, instead of applying the general CIP-007 standards to them. Using the previously referenced patch management system example, a standard for an application deployment or patch management system could be that the system must demonstrate methods to ensure the integrity of deployment packages to endpoints (authorization of deployments, validation of deployment content, and that's it).	

Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
The types of devices in the examples typically require Interactive Access to Cyber Assets, and as such are already in scope of the standard based on CIP-005 R2. A network communication centric identification is better suited to these types of assets.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
See our comments in #6 above. We believe the definition is too broad as written.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports Edison Electric Institute’s and NPCC’s comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

The proposed definition of CMS is more general than just those types of CMS associated with command and control of virtual resource environments. This takes the discussion beyond the scope intended for addressing virtualization technology in the context of CIP. If the SDT decides to include CMS applicability, the definition should be refined to include only virtualization or addressed in a new CIP standards modification project.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	No
Document Name	

Comment

Southern Company does not agree with the SDT’s approach to reference the CMS specifically as a type of applicable system in the CIP Standards. As stated in Question 6, CIP-010 change management is being administered for the BES Cyber Systems that are administered through these CMS systems. Also additional clarity would be required for how the definition would be used and why it would be an applicable system different than a PCA or other already in-scope Cyber Asset.

Likes 0	
Dislikes 0	

Response

Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC

Answer	No
Document Name	

Comment

We do not think you should differentiate CMS from EACMS. If anything, you should broaden the definition of an EACMS to include other central management and administration systems. Many of these systems perform both functions, which would only increase ambiguity.

Likes 0	

Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends the SDT consider that some tools (such as CMS) are not critical to the operation of the BES.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
ATC agrees with EEI’s comments that it is unclear how this new definition will be used and therefore it is also unclear why it would be referenced as a type of applicable system in the CIP standards.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
It is unclear how this new definition will be used and therefore it is also unclear why it would be referenced as a type of applicable system in the CIP standards.	
Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez

Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Additional clarification is needed on how this new definition will be used and why it would be referenced as a type of applicable system in the CIP standards. Specific examples are needed to clearly describe the context and how these devices will be used in the CIP environment.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
In practice, how does the definition of a CMS differ from that of an EACMS? How would the risks be mitigitated differently? Without any clear intent of how the SDT plans to implement a new defition, PacifiCorp cannot support the creation of one.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Kansas City Power and Light supports Edison Electric Institute’s Comments.	
Likes 0	

Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
See comments to question 6.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
It is unclear how this new definition will be used and therefore it is also unclear why it would be referenced as a type of applicable system in the CIP standards.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
No, as discussed above, AZPS respectfully submits that the development and creation of additional terms and asset classifications is unnecessary. All cyber assets (physical or virtual) can be classified in existing classification of Cyber Asset if it is modified as recommended in AZPS's response to Question #2. Hence, AZPS does not agree with or support the creation of a new definition for CMS or the use of such a term in the CIP Reliability Standards.	
Likes 0	

Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
The proposed CMS should be classified as its own applicable system to ensure controls specific to those Cyber Assets are required.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
DOminon agrees that this approach could lessen the risk of misidentifying these types of devices as they have a potential impact to BCSs within 15 minutes of their operation.	
Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Consistent with Exelon’s response to question 6 above, we support specific applicability; however, as long as the definition is sufficiently scoped to only be those “Centralized Management Systems” related to the tools to manage the virtualized environments.

Additionally, the informational posting states that the SDT is concerned with risks to the virtualized environment presented by the use of a centralized management system (CMS) to meet CIP requirements. It would be helpful if the CIP SDT would more fully explain what those risks are and the scope of CMS that require protections. The definition as presented could apply to any CMS used for general administration of existing BES Cyber Systems (e.g., configuration management, patching, etc.). We do not believe the SDT has provided a sufficient reason to extend CIP applicability to all CMSs, especially if those systems do not fall within CIP scope now because they do not qualify as BES Cyber Systems and are not associated with their PCAs, EACMS or PACS. The approach used should be clear in limiting the applicability of the CMS to virtualized environments.

Likes 0	
Dislikes 0	
Response	

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	

This will help reduce confusion over the classification of different types of systems and provide explicit direction for registered entities and auditors.

Likes 0	
Dislikes 0	
Response	

Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

A CMS is a vulnerable asset just like any other in a network, often more so as they are generally designed to be run on private, secured networks and are rarely the focus of as much security testing as other systems.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the SDT's approach to reference the CMS specifically as a type of applicable system in the CIP standards, assuming the SDT develops a clear definition for CMS. It provides clarity to the scope of systems that should be afforded protections but do not necessarily fall under the EACMS definition. SRP suggests adding criteria to determine a CMS and limiting the scope to the BES.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Clarification is necessary to consider EACMS, intermediate systems and other environments outside of the BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	Yes

Document Name	
Comment	
In examining virtualization, the SDT considered centralized management systems or consoles for these environments. These systems allow for the mass addition, deletion and modification of virtual machines and networks. Access to the control surface of a cyber system is known as the *management plane*. The management plane is where the virtual infrastructure is configured and managed by a limited group of administrators as opposed to the *data plane*. The data plane is where the end user's access to the virtual machine's business function takes place. To meet the security objective of protecting a BES Cyber System from threats in the data plane, the management plane should be isolated from the data plane. These types of controls are referred to as *out of band* management. The SDT is considering limiting the scope of management plane protection requirements to high and medium impact Control Centers because these environments contain the highest risk.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
It is the correct approach, but specific requirements need to be added to address the protection and management of CMS. They should be managed similar to EACM.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
While ITC agrees with protecting critical systems that can be compromised to affect the systems they manage, more determination needs to be made carefully regarding the controls for the proposed CMS system.	
Likes 0	

Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	

This type of systems are not addressed in the standard and represent risks that need to be addressed.

In examining virtualization, the SDT considered centralized management systems or consoles for these environments. These systems allow for the mass addition, deletion and modification of virtual machines and networks. Access to the control surface of a cyber system is known as the *management plane*. The management plane is where the virtual infrastructure is configured and managed by a limited group of administrators as opposed to the *data plane*. The data plane is where the end user's access to the virtual machine's business function takes place. To meet the security objective of protecting a BES Cyber System from threats in the data plane, the management plane should be isolated from the data plane. These types of controls are referred to as *out of band* management.

The SDT is considering limiting the scope of management plane protection requirements to high and medium impact Control Centers because these environments contain the highest risk.

Likes 0	
Dislikes 0	
Response	
Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	

Due to their potential impact on the assets they manage, it would be appropriate to have controls identified through requirements.

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name

Comment

This is an area some Responsible Entities have had difficulty with under the current Standards. Explicitly identifying CMS as a separate system type will provide needed clarity that these systems must be protected.

Likes 0

Dislikes 0

Response

David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer Yes

Document Name

Comment

Due to their potential impact on the assets they manage, it would be appropriate to have controls identified through requirements.

Likes 0

Dislikes 0

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer Yes

Document Name

Comment

Yes. Agree there are systems that may pose a risk to Cyber Assets if compromised that do not meet the strict definition of EACM.

In examining virtualization, the SDT considered centralized management systems or consoles for these environments. These systems allow for the mass addition, deletion and modification of virtual machines and networks. Access to the control surface of a cyber system is known as the *management plane*. The management plane is where the virtual infrastructure is configured and managed by a limited group of administrators as opposed to the *data plane*. The data plane is where the end user's access to the virtual machine's business function takes place. To meet the security objective of protecting a BES Cyber System from threats in the data plane, the management plane should be isolated from the data plane. These types of controls are referred to as *out of band* management.

The SDT is considering limiting the scope of management plane protection requirements to high and medium impact Control Centers because these environments contain the highest risk.

Likes 0

Dislikes 0

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

Centralized Management Systems are a huge issue for NIPSCO OT. We have wrapped a number of our CMS' into EACMS which causes a ton of grief for our operability. These suites of systems require special protections but not the same level as an EACMS. I agree with this definition as it identifies areas that are of significant security concern while potentially minimizing impacts to our operability. NIPSCO OT has taken a conservative approach with our management consoles and made all of them EACMS systems. This causes significant costs and difficult operability for my teams. I would encourage further development on this term and encourage that the requirements are placed somewhere between a TCA and an EACMS.

Likes 0	
Dislikes 0	

Response

Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

My concern, as stated, is that once you start down this road of including new concepts into a v5 CIP set of standards. Where does it end? I would recommend a fresh start and virtualization only definitions, security control, and auditing that are similar to other industries.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

Agree that these sytems represent a systemic risk and it is prudent to reconginze as such. There is concern though regarding what additional controls might be placed on a CMS, specifically their applicablitiy and feasbility given the many different types of CMS that might exist.

Likes 0	

Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
We agree with this approach to require the isolation between the data plane and the management plane. The required separation between the two plans will provide greater security and follows the same principal applied to “Seperation of Duties” concept.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Due to their potential impact on the assets they manage, it is appropriate to have controls identified through requirements.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

Likes 0

Dislikes 0

Response

Wesley Maurer - Lower Colorado River Authority - 1,5,6

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

It is BPA’s experience that there are inherent risks in centralized management systems’ span of control and privileged access to CIP-applicable Cyber Systems. BPA recommends that this be addressed in support of the security objective of protecting BES Cyber Systems from threats in the data plane by isolation of the management plane (out of band management).

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE recommends the SDT consider adjusting the existing EACMS definition, which has been applied (applicable systems) to the CIP Requirements already.

Likes 0	
Dislikes 0	
Response	

8. Do you agree with the SDT’s approach to require the isolation between the data plane and the management plane? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
The data plane already receives what’s considered the highest level or protection in the CIP standards. There would be little gained by separating the data and management planes.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Kansas City Power and Light supports Edison Electric Institute’s Comments.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
The data plan already receives what’s considered the highest level of protection in the CIP standards (likely a High Impact ESP). Little would be gained by elevating the protections of the management plane.	
Likes 0	

Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Further clarification is needed on the data plane and management terms, and the context in which they will be used.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The SDT’s intent with these new terms is unclear, including how they will be used.	
Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	No
Document Name	
Comment	
LCRA requests a definition of isolation and will then consider and vote accordingly.	
Likes 0	
Dislikes 0	
Response	

Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	
This is good practice. However, this may not always possible with some hardware. So, you should include “per Cyber Asset capability” and possibly allow for TFEs if this is required.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
Southern Company agrees with the SDT’s approach to require the isolation between the data plane and the management plane, but it is unclear at what level the SDT is asking the question. The data plane and the management plane are isolated by the nature of the configuration of the virtual system and the role authorizations which are provided for each. If the SDT is concerned with network level connectivity and that network access to administrative environments should only occur over separate physical networks or connections, then caution is required as not all systems or Cyber Assets can support physical out of band management. Even if limited to only Control Centers (as in Question 9), not every Cyber Asset in a Control Center can be administered out of band. This goes back to the issue in Question 1 where every requirement is expected to be applied to every device.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy agrees in principle, but we cannot agree entirely at this time without more information as to the direction of this approach. More information is needed as to what the SDT means by “isolation” at the physical and virtual level.	
Likes 0	

Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
This decision should be up to the entity. In-band management may be appropriate in a small environment. Some vendors also require in-band management in their reference architecture. The definition of a CMS includes systems such as patch management servers. Typically these communicate in-band to systems using built-in operating system mechanisms. If included this would involve creating a separate management plane for all systems, and additional work to segregate data and management planes. This architecture may not be supported by EMS vendors. Other devices have only a single network port and the data and management planes cannot be segregated. In some cases management systems are created specifically for high-risk systems. These management systems are treated at the same level and are used in band to manage a small number of devices.	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	No
Document Name	
Comment	
Out of band management is only one way to isolate the management of systems from user access. Dedicated management VLANs and perimeter and host firewall rules are effective at this, for example, and don't require out of band management to be an effective method of securing the administrative functions of a system.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
Answer	No
Document Name	
Comment	

The isolation of the two planes would only make sense in a mixed trust environment. These additional controls should be determined based on the increased risk to the BES due to the management of multiple BES Cyber Systems from a single source. The addition of the controls should not be based solely on the existence of the management plane. If the Entity chooses to not high watermark then the Entity must isolate. This isolation should not be required in all situations.

Virtualization brings new risks. I think this is one of them. These new risks need to be analysed and addressed.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG disagrees. The management plane should be addressed at the high water-mark. The management plane needs controls but, it doesn't necessarily have to be isolated from the data plane (this would mean that an entity would have to create a separate network). It should be sufficient that the management plane has controls which protect it from the data plane.

Likes 0	
Dislikes 0	

Response

Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6

Answer	No
Document Name	

Comment

We are concerned that the language would not allow for single plane management if the virtual system resides wholly within an ESP. Also there does not appear to be a distinction between EACMS and BES Cyber System.

We are also concerned that this approach would require entities to build a separate architecture to manage the data plane and management plane.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	No
Document Name	
Comment	
The language is too ambiguous to understand the requirements. Out of band management comes with many connotations when it comes to deployment methods. More specificity needs to be provided in the proposed requirement. For example, should console servers be deployed to provide out of band management? Would VLAN separation of management interfaces vs. non-managed interfaces be sufficient? All this is unclear in the proposed language.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	No
Document Name	
Comment	
LCRA TSC requests a definition of isolation and will then consider and vote accordingly.	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	No
Document Name	
Comment	
LCRA TSC requests a definition of isolation and will then consider and vote accordingly.	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes that proper separation of end-user and administrative capabilities is important in any information processing context. However, N&ST recommends against trying to develop new data / management plane isolation requirements in virtual environments unless the SDT can (a) reach consensus on a clear definition of what “isolation” means and (b) can identify specific examples, to be included in requirement statements, of approaches to achieving “isolation” that would satisfy the requirement(s).

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support the addition of a new conceptual framework for provision of security controls on a *management plane* and *data plane*. These concepts are new to NERC CIP, with potential for confusion and mis-interpretation by auditors and registered entities, as well as unforeseen special cases that do not fit the binary concept as presented.

Existing security controls applied to hypervisors and VMs are sufficient without the need for a new conceptual framework, through use of the definitions for Cyber Asset, BCS, and PCA including hypervisors, as previously commented. The management and data plane concepts would be useful to publish in guidance, rather than to requirement language. CenterPoint Energy suggests language in the guidance to explain the distinction between access controls to data that is accessible to authorized users of a system versus data isolated in a VM or container with authorized users of its own inaccessible to users of the host.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

While out of band management is a good practice, it should not be a requirement. There are other ways to segregate traffic. CIP does not require this for physical systems. If this is not requested for physical systems, then it should not be required for virtual systems. Additionally, the requirement should not be as specific as this may limit future technology. Stating “the data plane should be protected from the management plane” would be an alternative. Having specific ways to do this could be listed in the Guidelines and Technical Basis section.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

The description contained in the document was not clear enough to know the intent of the SDT. Without understanding the potential use of the approach outlined by the SDT, Dominion cannot support such a proposal.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

AZPS believes that the modification of the definition of Cyber Asset, coupled with the existing CIP requirements, affords sufficient differentiation between these planes and, therefore, as requirements become applicable, sufficient isolation – even where the co-mingling of CIP and non-CIP Cyber Assets on the same physical infrastructure – is present.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6

Answer	Yes
Document Name	

Comment

Due to their potential impact on the assets they manage, it makes sense to require isolation between the data plane and the management plane. AE requests more guidance on this issue. It is allowable for the management plane and data plan to coexist in the same environment so long as the environment is watermarked to the highest level of either plane.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

Clarification is needed if logical isolation is sufficient or if physical isolation is intended here. Either seems prudent however physical might be cost prohibitive for smaller virtualization setups. Perhaps there should be some manner of threshold for when this becomes necessary, for instance when the number of virtual cyber assets is some multiple greater than he underlying phyiscal hosts.

One factor that separation of the management and data plane does not address is the additional systemic risk posed by the physical hosts themselves, even with a segregated management plane. For instance, in the most simple case without physical reduancy to illustrate the point, if 10 physical cyber assets are converted to virtual machines on a single physical host, the cyber assets are still "leveraged up" 10:1 to a physical failure or to a direct cyber attack that quite possibly bypasses the management plane. This is a systemic risk not addressed by the data / management plane speration proposal.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	Yes
Document Name	

Comment

Reclamation supports the SDT’s approach to the isolation between the data plane and the management plane.

Likes 0	
Dislikes 0	

Response

Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Low impact facilities should not be in scope for virtualization.	
Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	Yes
Document Name	
Comment	
The isolation of the two planes would only make sense if the Cyber Assets in those planes were allowed to different required security controls apart from the associated impact level. These additional controls should be determined based on the increased risk to the BES due to the management of multiple BES Cyber Systems from a single source. The addition of the contols should not be based solely on the existance of the management plane.	
Likes 0	
Dislikes 0	
Response	
Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Yes. NIPSCO OT completed work to separate the management plane of the virtual environment in January 2017. This is a common IT best practice and should certainly be encouraged.	
Likes 0	
Dislikes 0	
Response	

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	Yes
Document Name	

Comment

Yes. Conforms with the principle of least privilege.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	Yes
Document Name	

Comment

Due to their potential impact on the assets they manage, it would be appropriate to require isolation. We request more information on this. It is allowable for the management plane and data plan to coexist in the same environment as long as that environment is watermarked to the highest level of either.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

Isolation between the data traffic and the control traffic will improve security, albeit at the cost of added complexity. This tradeoff is probably worthwhile in larger Control Centers, but may not be feasible at the low impact level at this time.

Likes 0	
Dislikes 0	

Response

Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
This is appropriate especially if you consider this to be a form of iLo or some other Out of band management (OOBM) function. OOBM functions that touch BES Cyber Assets should have a separate network in the PSP in order to properly secure it.	
Likes 0	
Dislikes 0	
Response	
Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Due to their potential impact on the assets they manage, it would be appropriate to require isolation. We request more information on this. It is allowable for the management plane and data plan to coexist in the same environment as long as environment is watermarked to the highest level of either.	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
SCE&G would like for it to be separated. As an organization, we're currently performing isolation between the data plane and the management plane.	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	

Answer	Yes
Document Name	
Comment	
Virtualization brings new risks. I think this is one of them. These new risks need to be analysed and addressed.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP agrees with that it is appropriate to require isolation between the data plane and management plane. AEP recommends the SDT identify procedural controls related access request and access management practices rather than technical controls which may not be readily demonstrable.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
This is a standard approach to security separation to limit scope and impact	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	

Comment

As indicated in our comment 5, above, we are concerned that some of the concepts and approaches being presented may not reflect the full range and diversity of virtual systems. Please carefully word any requirements to avoid tying obligations to one particular virtualization concept or approach.

Likes 0	
Dislikes 0	

Response

Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

The risk inherent with the management plane is elevated because of the potential impact of a malicious or non-malicious change to the device. The approach to separate the management and data planes is fundamentally sound. The issue that must be addressed, however, is the implementation used to separate these two planes. For example, utilization of logical separation via VLANs creates an easy and simplistic method for the separation. However, this is not necessarily the most secure method of separation. Likewise, the use of VLANs with a two byte tag to the header is not secure; this tag can be modified by an adversary through various techniques. When looking at the current state of technology and discussing physical separation, what does this imply? For example, if two devices that should be physically separated were to be connected to a SDN switch (e.g., SEL-2740S) there is no 'physical' connectivity between the devices. The switch has no capability to route/forward traffic between these two devices until an appropriate instruction (e.g., Match/Action rule in the case of OpenFlow) is sent to the switch. With SDN technology and SDN Ethernet switches, virtual separation equals physical separation.

Language should be clear and concise enough to define a separation between the management and data planes where adversarial techniques cannot cause routing or access of communication between these two planes. Specifically, the language stating OOB (Out of Band) and other technology that allows for the equivalent of OOB.

SDN offers the capability to isolate flows within the packet forwarding device (Ethernet switch). In this case, it is not necessary to populate the header or payload of the Ethernet frames with switching isolation data. The SDN switch should have a secure encrypted command channel to the switch's controller to prevent a man-in-the-middle (MiM) type of attack that would allow it to receive instructions from an illegitimate assigned controller. This type of solution allows the use of the same physical network infrastructure and the policy and flow rules of the SDN to create the separation in a highly secure manor.

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF

Answer	Yes
Document Name	

Comment

With the addition of a “where technically feasible” PJM agrees with the SDT’s approach.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

Exelon would like to see this addressed in the Guidance and Technical Basis section. Additional guidance can help by providing examples of data plane vs. management plane and how they could be adequately isolated. We interpret this isolation to include limiting the ability of any data plane to expand permissions into the underlying management plane. This is a standard security control within virtualized system management. There are also vulnerabilities that would constantly challenge this isolation – which could position a compliant solution one day as non-compliant the next.

Intermediate systems and other assets that are not completely located within an ESP benefit from data plane/management plane isolation. However, the systems that are entirely contained within an ESP may not benefit from the isolation at the cost of additional logical and physical complexity to provide that isolation. Any additional guidance should clearly address only the case where a virtualized environment is not completely contained within an ESP, and not imply isolation requirements for systems already contained entirely within an ESP (and protected accordingly).

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

BPA agrees with the SDT’s proposal to require isolation between Data Plane and Management Plane for centralized management systems when system capability allows and risk justifies it. BPA cautions the SDT against overly rigid prescriptions for providing isolation. Combinations of other controls may afford the same or better protection in a particular circumstance. When the use of automated tools can improve security and manageability, it is important to avoid discouraging automation with overly burdensome compliance requirements.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	

Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

9. Do you agree with limiting the applicability to high and medium impact Control Centers? Please provide your rationale.

(Refer to the Unofficial Comment Form for more information on this question)

Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
Exelon generally agrees that the greater risk exists at high and medium Control Centers. However, what is the potential applicability to other medium impact assets where virtualization might be considered? We also suggest addressing how virtualization might allow for the aggregation of multiple Low Impact Systems to the point where there is a much greater potential impact to the BES than from each individual Low Impact device or System. (Reference this Vulnerability - https://www.theregister.co.uk/2017/03/31/researchers_steal_data_from_shared_cache_of_two_cloud_vms/)	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Tri-State would like the SDT to provide more information regarding the use of virtualization on EACMs and PACS. As written, the SDT is only covering assets within the ESP, however, virtualization is also being used for EACMs and PACS systems. We anticipate there will be some requirements to incorporate this type of utilization. Could the SDT please speak to this?	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

SDN's high degree of repeatability drives economic viability in smaller installations. Given that even low-priority installations may be an attack target, it would seem wise to secure them as well.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

Control centers are certainly important and are the minimum level to include. I would argue that Medium impact sites that utilize virtualization also need to be included as they have isolated impact that is significant. Hence, this should be applied to all High and Medium impact sites and their associated PCAs and EACMs.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

The impact level already determines that there are three risk levels, High, Medium and Low. The existence of “external routable connectivity” is an additional qualifier. It seems that the SDT’s plan is to use “Control Center” as another qualifier. It is understood that a Control Center is at a higher risk because of its span of control. This increased risk has already been addressed in the application of the CIP-002-5.1 criteria.

Likes 0	
Dislikes 0	

Response

Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6

Answer	No

Document Name	
Comment	
No comment on this question.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and ISO-NE	
Answer	No
Document Name	
Comment	
The impact level already determines that there are three risk levels, High, Medium and Low. The existence of “external routable connectivity” is an additional qualifier. It seems that the SDT’s plan is to use “Control Center” as another qualifier. It is understood that a Control Center is at a higher risk because of its span of control. This increased risk has already been addressed in the application of the CIP-002-5.1 criteria.	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Sempra - San Diego Gas and Electric - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	
It should also include all high and medium BES Cyber Systems with ERC, not just at control centers.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	

Comment	
Definitions and frameworks are required to give guidance to all levels of systems. A VLAN management system that manages network devices at many transmission stations should also be in scope of the protection.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
See our comments to question 8. We agree in principle, but need more information on direction headed before we agree with the approach at this time.	
Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
The impact level already determines that there are three risk levels, High , medium and low. The existance of “external routable connectivity” is an additional qualifier. It seems that the SDT’s plan is to use “Contol Center” as another qualifier. It is understood that, a Control Center is at higher risk because of its span of control. This increased risk has already been addressed in the application of the CIP-002-5.1 critera.	
Likes 0	
Dislikes 0	
Response	
Joseph Mosher - EDF Renewable Energy - NA - Not Applicable - WECC	
Answer	No
Document Name	

Comment	
We do not think that this should be required as it is not possible in all situations.	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 1,5,6	
Answer	No
Document Name	
Comment	
LCRA feels that applicability should be limited to High Impact Control Centers.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS recommends the SDT provide the industry with clarity on this topic by not limiting the application of virtualization or requirements applicable to virtualized assets to a given BCS type. This will ensure that both the security and reliability objectives of the reliability standards are met and that points of confusion, potential for human error, etc. with respect to virtualization are reduced. AZPS is concerned that the limitation of applicability could introduce complexity, confusion, and ambiguity into the applicability of the requirements to virtualized assets especially where there is co-mingling of CIP and non-CIP assets that have been assigned different impact ratings. For example, if there is a management system that is virtualized across generating units which range from medium impact to non-CIP or low impact or that is virtualized physical locations, the requirements that are applicable to the shared portions of the Cyber Assets may become unclear for both Registered and Regional Entities.	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA agrees with limiting applicability only to those facilities such as High and Medium Control Centers with the highest level of risk is reasonable, and there may be exceptions to those as well. Combinations of other controls may afford the same or better protection in a particular circumstance.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
The applicability should be based on risk to the stability of the BES and not an arbitrary classification.	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Yes. Low impact BESCS have limited controls already. Not sure how this would fit into their requirements.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Expanding the applicability to medium impact BCS would cause an undue burden on entities and could affect reliability.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
High and medium impact Control Centers pose the greatest risk to the BES.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The impact of the realized threat would not justify the cost in a low impact environment.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes

Document Name	
Comment	
If isolation standards are put in place, they should be quite limited in scope. Specifically, to where they have had actual, proven effectiveness, and where implementation is not prohibitive in cost and effort when compared to the security gained.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP agrees that limiting applicability to high and/or medium impact Control Centers is appropriate due to their associated risk. AEP is unclear if the SDT is suggesting that this guidance limit applicability only to BCS or other related Cyber Systems such as EACMS or PACS as they are just as likely to be virtualized.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
NRG does not have any comments on this.	
Likes 0	
Dislikes 0	
Response	
Lee Maurer - Oncor Electric Delivery - 1	
Answer	Yes

Document Name	
Comment	
This should not be applied to low impact due to the lesser risk they present to the BES.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
See the answer to (8) above.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG supports Edison Electric Institute's comments.	
Likes 1	PSEG - PSEG Fossil LLC, 5, Kucey Tim
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2 - MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	

*It should not be required to apply these me*asures to low impact assets due to the lesser risk they present to the BES.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	Yes
Document Name	

Comment

Yes. Agree with risk assessment.

Likes 0	
Dislikes 0	

Response

Sarah Gasienica - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

Yes. The cost of separating management plane traffic is often difficult with equipment rolled out to low impact sites. The risk is typically very minor and the costs are typically significant. The return on investment is just not present and the risks do not justify this need.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

There is significantly more risk at control centers because of the type of connectivity and number of devices they have that are capable of Multi-Tenancy and out of band management. Enforcing this control at substations would be impractical in many configurations.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	Yes
Document Name	

Comment

Southern Company agrees with limiting the applicability to High and Medium Control Centers. These assets pose the highest risk to the BES and are in the locations with the primary need for virtualization technologies. However, see the issue on Question 8 as location or facility type alone does not mean the technical capability of all Cyber Assets within it are at a certain level.

Likes 0	
Dislikes 0	

Response

Warren Cross - AEP - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

Low impact facilities should not be in scope for virtualization. Smaller entities are having a hard enough time adjusting to the current v5 requirements. If a Low impact facility wants to move into a virtual work then that is their option. NERC had been so opposed to virtualization for so long, it will take some time for new comers to the technology to become proficient in supporting it.

Thank you for your time and consideration to comment.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	Yes
Document Name	
Comment	
Reclamation supports limiting the applicability to only high and medium impact Control Centers.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
This seems prudent espeically given this initiative is in the early stages. Adding controls to Low systems might better be kept until after experience with controls on high and medium systems is more developed. However, consideration should be given to situatios where Low Impact BCAs are managed with the same CMS as used for High and Medium BCAs such that controls intended for high and medium related CMS do not unduely carry over as requirements on the managed low impact cyber assets in such cases.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
High and medium impact Control Centers pose the greatest risk to the BES.	
Likes 3	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Great Plains Energy - Kansas City Power and Light Co., 1,3,5,6, Webb Douglas; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
These areas carry the greatest level of risk (and are certainly the most likely to see virtualization in use).	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Darnez Gresham, N/A, Gresham Darnez
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Kansas City Power and Light supports Edison Electric Institute’s Comments.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Limiting the applicability to high and medium impact BCSs at Control Centers makes sense due to the lesser risk posed by low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Watkins - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes

Document Name	
Comment	
High and medium impact Control Centers pose the greatest risk to the BES. Medium facilities such as a substation facility will most likely only effect one facility vs. the many facilities managed by a Control Center.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 2 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Concepts for Virtualization and Definitions

Do not use this form for submitting comments. Standards Balloting and Commenting System (SBS) to submit comments on **Project 2016-02 Modifications to CIP Standards Virtualization in the CIP Environment.** The electronic form must be submitted by **8 p.m. Eastern, Thursday, November 2, 2017.**

Additional information is available on the project page. If you have questions, contact Katherine Street (404) 446-9702 or Mat Bunch (404) 446-9785.

Background Information

The Standard Drafting Team (SDT) for Project 2016-02 Modifications to CIP Standards continues to work to address transferred issues from the Version 5 Transition Advisory Group (V5 TAG). The V5 TAG consisted of six volunteer Responsible Entities who worked with NERC and the Regional Entities to implement the CIP Version 5 standards in an accelerated time frame. During the implementation study, study participants focused on the technical solutions and processes needed to meet the standards. As a result of this effort, issues were identified with the definition of Cyber Asset as well as the use of virtualization. These issues were documented in CIP V5 Issues for Standard Drafting Team Consideration.

The SDT has conducted outreach to industry on the concepts of virtualization through webinars that are published on the Project 2016-02 Modifications to CIP Standards related files page. To address the topics of the Cyber Asset definition and virtualization, the SDT has developed concepts for which we are seeking informal comment to gather further input from stakeholders. In reviewing these concepts and risks, it became clear that other areas may need to be adjusted to provide a clearer categorization of assets and applicable requirements to address the risk of virtualization.

As a result of this work, this comment form introduces new concepts which may result in the development of new requirement language, new definitions, and modifications to existing definitions. SDT proposes these concepts to:

1) Refine terms related to virtualization, such as Cyber Asset and Centralized Management System (CMS).
2) Improve areas in the current CIP Standard requirements that might hinder the adoption of virtualization technologies for BES Cyber Systems and other related systems;
3) Address areas of new cybersecurity risks, technological concepts, and techniques introduced with virtualization technologies; and
4) Clarify the context of virtualization technologies and mixed physical and/or virtual environments where advancing technologies have blurred boundaries or made legacy approaches obsolete.

The concepts noted within this informal comment form are not an obligation for Responsible Entities to implement virtual technology. The target audience for this informal comment form are those Responsible Entities that have implemented or are planning to implement virtual technology.

Concept 1: Modifications to allow use of secure multi-instance environments

Cyber Asset Definition

The V5 TAG implementation study noted issues with the use of the term Cyber Asset in the context of virtualization. In virtual environment, how does the construct of a virtual system align to the definition when the various components are distributed across a vast array of infrastructure components? Additionally, the V5 TAG requested that the SDT clarify the intent of “programmable” by considering such factors as whether a device is merely configurable, its executable code is not field upgradable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc.

In April 2017, the SDT received comment from industry that indicated that the definition of Cyber Asset would benefit from clarification how it relates to physical and virtual systems. Many comments also indicated that through broader industry implementation, issues with the meaning of “programmable” had been resolved and the definition of Cyber Asset did not need to be modified to address this. Additionally, ERO Enterprise-endorsed Implementation Guidance exists on the term "programmable".

Due to the foundational nature of the Cyber Asset definition as well as the comments received in April 2017, the SDT seeks comment on the following conceptual definition of Cyber Asset in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Current:

Cyber Asset:

Programmable electronic devices, including the hardware, software, and data in those devices.

Redline

Cyber Asset:

A programmable electronic physical or virtual device~~s~~, including the hardware, software, and data in th~~os~~e device~~s~~. Each virtual machine and host is a distinct device.

Clean

Cyber Asset:

A programmable electronic physical or virtual device, including the hardware, software, and data in the device. Each virtual machine and host is a distinct device.

1. Do you agree that the proposed change to the Cyber Asset definition makes it inclusive of both physical and virtual devices, including treatment of each virtual machine and hypervisor? If you do not agree, please provide rationale to support your position.

   ☐ Yes
   ☐ No
   Comments:

2. Do you agree that the term programmable in the Cyber Asset definition does not need further clarification at this time? If yes, please provide rationale to support your position.

   ☐ Yes
   ☐ No
   Comments:

3. If programmable does need further clarification, how would you prefer it to be addressed? Use comments to detail necessary definition changes or guidance that could be developed.

   Comments:

Centralized Management Systems (CMS)

As the SDT worked through issues related to virtual systems, it became clear that there was no straightforward way within the current CIP Standards to adequately address the risk of systems used to manage virtual environments. Management systems in virtual environments, through their consolidated interfaces and automation, can modify and delete entire infrastructures including virtual servers, networks, and storage. Given the broad capabilities of management systems in a virtual environment, they present specific and significant risk to the reliability of the BES Cyber Systems associated with those management systems.

The SDT considered several options to address the risks of management systems such as grouping management systems into the existing EACMS definition. This, however, would place these assets inappropriately in the EACMS category when they do not perform access control or access monitoring. Using the EACMS category in this manner creates a one-size-fits-all approach to requirements that does not consider the degree of risk or technical constraints posed by the particular system. For example, a system that only monitors and logs access does not pose the same level of risk as a management system for a large virtualized Control Center with the capability to modify or delete a complete infrastructure. Technical controls to mitigate the risk may differ depending on the capabilities of the management system. An electronic access monitoring system presents a risk of leaking BES Cyber System Information; an electronic access control system presents a risk of unauthorized access to, or modification of, a BES Cyber System’s operational parameters; and a management system presents a risk of unwanted or unintended modification or deletion of a complete infrastructure.

Proposed requirements related to this definition are detailed below.

The SDT determined a more appropriate option was to create a new definition for Centralized Management System (CMS) and apply appropriate and specific security requirements. The SDT seeks comment on the following conceptual definition of Centralized Management System in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Centralized Management System (CMS):
A centralized system used for administration or configuration of BES Cyber System(s) through which the configuration of the BES Cyber System can be altered.

4. Do you agree with the proposed definition of Centralized Management Systems (CMS)? If not, please provide rationale to support your position.

   ☐ Yes
   ☐ No
   Comments:

Virtualization Terms and Requirements

The foundational pieces have now been set for the use of virtualization solutions. However, these solutions still pose risk. These risks and the nature of virtual systems may require some modifications to Standards. The concepts being proposed include additional access control and separation of the management plane from the data plane. This can help to prevent users of the applications on a virtualized system gaining access to the management system that can modify and delete the underlying infrastructure including virtual servers, networks, and storage.

The SDT uses the terms “instance” and “multi-instance” within the proposed requirements below. For the purposes of these proposed changes, the SDT intends for “instance” and “multi-instance” to be understood as:

- Instance: Discrete organizational environments with specific privileges or security levels, consisting of functions that consume resources from the shared infrastructure. Instances are logically isolated but physically interconnected.
- Multi-instance: An environment where a shared infrastructure provides containers for more than one instance.

In reviewing the risks that are unique and inherent to the use of virtualization technologies, the SDT identified the following risks:

1) Shared infrastructure,
2) Span of control, insider threats, and lateral privilege expansion,
3) Misconfiguration, excessive privileges, and capability of administrators, and
4) Escalation of privilege.

The SDT proposes the following definition and requirements in support of the use of virtual technologies.

Electronic Security Zone (ESZ)

The SDT contends that the Electronic Security Perimeter (ESP) definition does not accurately describe the proper isolation of virtual systems within shared infrastructure. Details of the analysis are captured in network isolation portion of the industry webinar presented on March 21, 2017. To address the concerns noted, the SDT seeks comment on the following conceptual definition of Electronic Security Zone (ESZ) in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Electronic Security Zone:
The area defined by the logical separation of one or more Cyber Asset(s).

5. Do you agree that the proposed definition of ESZ more adequately applies to proper isolation of multi-instance environments, regardless of OSI layer? If not, please provide a rationale to support your position.

   ☐ Yes
   ☐ No
   Comments:

6. Do you agree that the proposed definition of ESZ would aid the development of future CIP Standards by providing a more relevant level of separation? If not, please provide a rationale to support your position.

   ☐ Yes
   ☐ No
   Comments:

New Requirement CIP-005 Requirement 1, Part 1.6

The SDT proposes a new requirement part 1.6 for CIP-005 Requirement R1. This requirement part is for Responsible Entities to implement one or more Electronic Security Zones (ESZ) to meet the security objective of separating the management plane and the data plane of high and medium impact BES Cyber Systems in a multi-instance environment. Part 1.6 would also require Responsible Entities to implement one or more ESZs to meet the security objective of protecting the infrastructure associated with high and medium impact BES Cyber Systems in a multi-instance environment by limiting access to the Centralized Management Systems using a management plane ESZ.

Responsible Entities maintain the flexibility for grouping by cyber system function, by risk, by type of applicable security controls, or other logical groupings. The ESZ contains a distinct subset of the Responsible Entity's Cyber Assets. These are characterized as requiring (or benefiting from) similar security controls and separation from other distinct Cyber Assets. Properly implemented ESZs can limit damage and impact to availability to other surrounding ESZs, specifically by helping protect against span-of-control risks, insider threats, and lateral privilege expansion.

Again, the requirement would only be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS.

Part 1.6:
Logically separate all Applicable Systems into defined groups of one or more Cyber Asset(s) to achieve the objective of mitigating the risks of span-of-control, insider threats, and lateral privilege expansion. At a minimum:
1. The management plane and the data plane of the applicable BES Cyber System shall be separated;
2. The CMS of the applicable BES Cyber System shall be separated from its data plane

7. Do you agree that the proposed CIP-005 Requirement R1, Part 1.6 provides sufficient security controls for the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS to reduce the stated risks inherent to virtualization? If not, please provide a rationale to support your position.

   ☐ Yes
   ☐ No
   Comments:

New Requirement CIP-005 Requirement 1, Part 1.7

Similarly to CIP-005 Requirement R1, Part 1.3, the SDT proposes new requirement Part 1.7. Part 1.7 requires Responsible Entities to identify, control, and explicitly allow only necessary inbound and outbound communication between ESZs of high and medium impact BES Cyber Systems residing in a multi-instance environment. Part 1.7 would be added to CIP-005 to reduce the risks inherent to virtualization related to misconfiguration, excessive privileges, capability of administrators, as well as information protection and data leakage.

The requirement would be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s).

Part 1.7:
Implement technical controls that enforce separation between ESZs by allowing only necessary inbound and outbound communication between the separated Cyber Asset(s) residing in a multi-instance environment.

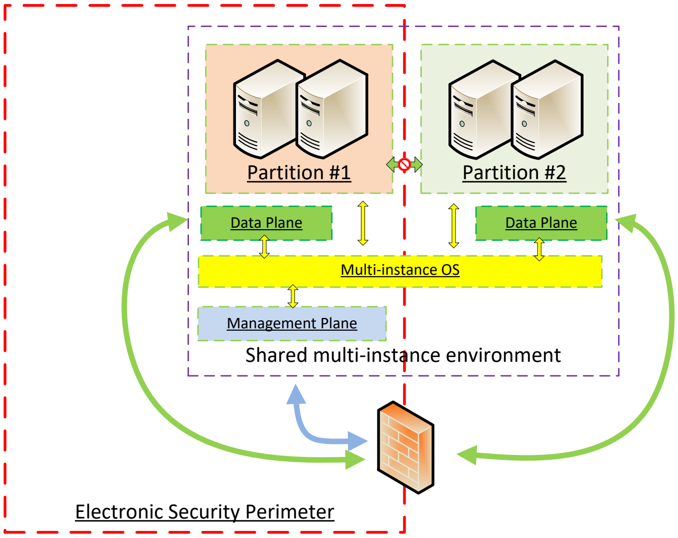
8. Do you agree that the proposed CIP-005 Requirement R1, Part 1.7 provides a necessary security control to the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s) to reduce risks inherent to virtualization? If not, please provide a rationale to support your position.

   ☐ Yes
   ☐ No
   Comments:

New Requirement CIP-005 Requirement 1, Part 1.8

Through the SDT work on virtualization, situations have been identified where a Responsible Entity may choose to share the same system infrastructure between applicable Cyber Assets and other programmable devices. As the footprint of cyber assets outside the scope of the CIP Standards in an organization might be significantly larger in size from the Cyber Assets in scope of the CIP Standard, a Responsible Entity may invest in its IT infrastructure with greater capability and more robust features. As presented in the third webinar on virtualization, this is particularly true with storage virtualization implementations. Under certain circumstances, leveraging enterprise infrastructure solutions will provide a better security posture for applicable Cyber Assets. Part 1.8 has been drafted with the objective of allowing such leverage as long as controls mitigating the additional risks are implemented.

A CIP Standard requiring the complete physical separation of applicable Cyber Assets and other programmable devices might adversely affect the overall security posture and reduce operational efficiency for the Responsible Entity through unnecessary expense and complexity of processes or technical implementation. Security controls exist to manage secure logical separation in multi-instance environments and there are operational benefits to sharing a common infrastructure as well. Technological advancements are often coupled with new security mechanisms which often benefit legacy infrastructure.



The diagram above shows an example of a shared multi-instance environment. The green arrows in the diagram represent the data communication. To exchange data between Partition 1 and 2, communication has to go through an EAP represented in the diagram by a firewall. The blue arrows in the diagram represent the management communication. In order to manage Partition 2, or any Cyber Asset hosted by the multi-instance environment and outside the ESP, IP communication to the management plane from outside the ESP has to go through the EAP since the management plan of shared multi-instance environment has to reside inside the ESP. The yellow arrows in the diagram represent the resource management activities performed by the multi-instance operating system necessary to ensure separation of data plane and management plane as well as partitions between Cyber Assets inside the ESP and Cyber Assets outside the ESP.

The SDT proposes CIP-005 Requirement 1, Part 1.8 to provide protection where the infrastructure used in a multi-instance environment is shared between applicable Cyber Assets and other programmable devices. This allows Responsible Entities to leverage the investments and protection of infrastructure shared between applicable Cyber Assets and other programmable devices. The requirement would be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s).

Part 1.8:
When an infrastructure is shared between BES Cyber Systems and other Cyber Assets not part of a BES Cyber System:

1. The BES Cyber System, the management plane of the shared infrastructure, and any hosted Cyber Assets not part of a BES Cyber Systems shall all be separated; and
2. Communications between the BES Cyber System and any hosted Cyber Assets not part of a BES Cyber System shall all be denied by default

9. Do you agree that the proposed CIP-005 Requirement R1, Part 1.8 provides sufficient security control to reduce the risks associated with shared multi-instance environments? If not, please provide a rationale to support your position.

☐ Yes
☐ No
Comments:

New Requirement CIP-005 Requirement 3, Part 3.1

In reviewing the risks associated with communications in a virtual environment, the SDT identified a gap with remote access used to perform CMS functions. These communications using a CMS do not align appropriately to Interactive Remote Access. Tasks may be performed from outside the ESP that are a blend of interactive and automated tools, allowing for misinterpretation and unjustified relaxation of security mechanisms required for Interactive Remote Access. Using jump servers to perform CMS functions might not be the most effective or the most secure. Also, remote access to a Cyber Asset inside an ESP could benefit from other methods besides Interactive Remote Access for performing CMS functions.

CIP-005 Requirement R3, Part 3.1 allows for a new type of remote access to be used to perform CMS functions from outside of an ESP. Part 3.1 allows the CMS function to be performed outside an ESP using an access method other than an Intermediate Systems to fix the gap that may exist between Interactive Remote Access and system-to-system communication. It does this by introducing requirements that are commensurate with the risk inherent to the management function in a multi-instance environment.

The SDT proposes new requirement CIP-005 Requirement 3, Part 3.1. Part 3.1 would be applicable to high and medium impact BES Cyber Systems.

Part 3.1:
Require authentication, integrity and non-repudiation controls for all sessions initiated outside of the ESZ, whether user initiated or system-to-systems communications, used to perform CMS functions.

10. The SDT asserts that the proposed CIP-005 Requirement 1, Part 3.1 provides additional security controls for remote access when performing CMS functions. These are necessary to reduce the risk associated with remote access to multi-instance environments. Do you agree with this assertion? If not, please provide a rationale to support your position.

    ☐ Yes
    ☐ No
    Comments:

11. Should the gap between Interactive Remote Access and system-to-system communication that was exposed by the examination of the risks inherent to virtualization be addressed for systems other than high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS? If not, please provide a rationale to support your position.

    ☐ Yes
    ☐ No
    Comments:

New Requirement CIP-004 Requirement 4, Part 4.5

The SDT has identified “too much privilege” as an inherent risk in virtualization. This risk can be reduced by adding controls in CIP-004. Limiting of the privileges granted to the minimum necessary is only present in the guidance. It is not a requirement. This security risk can be mitigated, however, by implementation of least privilege access and separation of duties in the requirement language. This means fewer people get high level privileges, and no single individual gets privileges that are too broad. For efficiency, it can be implemented via role-based access control (RBAC), which requires an initial effort to define roles properly. But also provides an opportunity for internal review of the span-of-control risk. Role-based access control and separation of duties are both available in virtual environments. Implementation of RBAC varies by vendor but is generically the same in principle.

The SDT proposes new requirement CIP-004 Requirement 4, Part 4.5. Part 4.5 would be applicable to high and medium impact BES Cyber Systems.

Part 4.5:
The Responsible Entity shall document and implement process(es), except under CIP Exceptional Circumstances, to authorize electronic and unescorted physical access to BES Cyber Systems and BES Cyber

Systems Information that implements the principles of need-to-know, least privilege, and separation of duties as determined by the Responsible Entity, as per system capability.

12. The SDT asserts that the new proposed CIP-004 Requirement R4, Part 4.5, provides additional security control to the electronic and unescorted physical access to multi-instance environment processes which reduces the “too much privilege” risk inherent to virtualization which has been identified. Do you agree with this assertion? If not, please provide a rationale to support your position.

    ☐ Yes
    ☐ No
    Comments:

Concept 2: Modifications to the EACMS definition

As noted above, the SDT reviewed the scope of the current definition, the requirements, and risk of the types of assets contained within EACMS. The current construct does not differentiate controls based on the functionality and risk of the system. The current construct does, however, create what is known as the “hall of mirrors” effect. Specifically, there may be some types of EACMS that should be required to be inside an ESP and behind a firewall. An example could be the management system of a firewall that is categorized in such a way that it must reside within an ESP. That requirement, however, cannot exist for all EACMS because a firewall is itself an EACMS. Without defining a new category, the result would be that every EACMS would need to be inside an ESP and therefore protected by another EACMS. This creates the recursive "hall of mirrors" effect.

There are a number of systems that both monitor and provide part of the solution of controlling access, but do not actually control traffic at the point of entry. These devices or systems may or may not benefit from being inside a protected boundary, or they may form part of the strategy that protects BES Cyber Assets. The technical means of implementing some multi-part systems may require components to be outside, or span the ESP.

To address this, the SDT proposes breaking up the EACMS categorization of applicable systems by function so that the appropriate requirements for each can be applied. The SDT does not, however, want to create a reclassification and documentation exercise for Responsible Entities who would not see benefit and would try to create a way for those Responsible Entities to continue to use EACMS with no changes. There are also other options in addition to these two.

Electronic Access Control System (EACS)

The SDT seeks comment on the following conceptual definition of Electronic Access Control System in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Electronic Access Control System (EACS):
Cyber Assets that perform electronic access control of the BES Cyber Systems. This includes Intermediate Systems.

An Electronic Access Control System performs authentication and authorization of traffic or users. This is the “gatekeeper” function or the classic authentication and authorization functions of standard AAA. In many cases these systems do not perform any active filtering of the traffic passing through any particular interface. The primary duty of EACS is to authenticate and authorize. EACS move beyond the risk of unauthorized access to meta-information about an environment, to unauthorized access to BES Cyber Systems and modification of their operational parameters.

Electronic Access Gateway (EAG)

The SDT seeks comment on the following conceptual definition of Electronic Access Gateway in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Electronic Access Gateway:
Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s). The Electronic Access Gateway also hosts the EAP(s).

An Electronic Access Gateway hosts the EAP and performs the active function of filtering or forwarding traffic at the demarcation point (boundary protection). Primarily, these are firewalls and routers that perform gateway functions at the layer 3 ESP boundary demarcation point.

Electronic Access Monitoring Systems

As technologies and cyber attacks advance and become more complex, Responsible Entities are becoming increasingly interested in collecting and correlating electronic access monitoring events across their enterprises. This broad-based information collection provides Responsible Entities with more visibility into emerging threats and trends. Responsible Entities can then analyze and share this information more readily and take action to improve the overall cybersecurity and reliability of the BES through early detection of compromise.

Under the currently effective CIP Reliability Standards, if a Responsible Entity uses enterprise wide electronic access monitoring tools, the Cyber Assets used to perform the monitoring may meet the definition of EACMS and become subject to the CIP Reliability Standards applicable to EACMS. This may discourage or prevent Responsible Entities from using enterprise wide electronic access monitoring due to the device level requirements of an EACMS. Responsible Entities may be discouraged from providing and correlating security events across enterprise and control networks, even though cyber-attacks against control systems could enter through business networks. The SDT concludes there is value in correlating security events across both control and enterprise networks.

The SDT proposes that the information within the electronic access monitoring systems should be protected as a BCSI repository, rather than having the system categorized as an EACMS. The systems performing electronic access monitoring are used to monitor and collect information about BES Cyber Systems or Electronic Security Perimeter(s) and pose a risk of information leakage. These monitoring systems are not used to control access to the BES Cyber Systems or Electronic Security Perimeter(s). The monitoring function has been in scope of the EACMS definition due to the sensitivity of certain information that may be collected. The proposed change is to treat the data collected through the monitoring capability as BCSI rather than having the monitoring systems categorized as EACMS. This change will enable Responsible Entities to better leverage enterprise-wide monitoring to improve overall situational awareness, and in the process more proactively address security events.

This will result in improved security and reliability. This does not change a Responsible Entity's obligations to monitor under CIP-007 R4.

To transition electronic access monitoring from EACMS to BCSI, the SDT seeks comment on the following conceptual modification to the definition of BES Cyber System Information in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Clean:
BES Cyber System Information:
Data about the BES Cyber System that is processed, organized, structured, or presented in a context that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.

BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to gain unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual or collections of IP addresses without context of location and purpose, ESP names, individual security logs, or policy statements.

Examples of BES Cyber System Information may include, but are not limited to: security procedures, collections of security logs, or security configuration information about BES Cyber Systems, Physical Access Control Systems, Electronic Access Control Systems, Electronic Access Gateway Systems, Centralized Management Systems, and Electronic Access Control or Monitoring Systems that are not publicly available; and network topology with network addresses of the BES Cyber System.

Redline:
BES Cyber System Information:
Data ~~Information~~ about the BES Cyber System that is processed, organized, structured, or presented in a context could be used to gain unauthorized access or pose a security threat to the BES Cyber System.

BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual or collections of IP addresses without context of location and purpose, ESP names, individual security logs, or policy statements.

Examples of BES Cyber System Information may include, but are not limited to:~~,~~ security procedures, collections of security logs, or security configuration information about BES Cyber Systems, Physical Access Control Systems, Electronic Access Control Systems, Electronic Access Gateway Systems, Centralized Management Systems, and Electronic Access Control or Monitoring Systems that is not publicly available ~~and could be used to allow unauthorized access or unauthorized distribution~~; ~~collections of network addresses~~; and network topology with network addresses of the BES Cyber System.

Current:

BES Cyber System Information:

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

Proposed Requirements Related to EACMS Changes

Based on the concepts presented above, the table below lists the current requirement scope of EACMS and those proposed for CMS, EACS, and EAG. In the table below, the "X" indicates where the requirement currently applies to the system category in the Applicable Systems column of CIP Standards. The "+" sign indicates an additional requirements being considered to address risk for that specific system category in the Applicable Systems column of CIP Standards. To the extent that there is no difference in requirement applicability, the SDT would look to consolidate the terms into as few classifications as necessary.

Please keep in mind that the SDT does not want to create a reclassification and documentation exercise for Responsible Entities who would not see sufficient benefit and would look to create a way for those Responsible Entities to continue to use EACMS with no changes.

Requirement	EACMS	CMS (+)	EACS (+)	EAG (+)
CIP-004 R1.x		+	+	+
CIP-004 R2.x	X	X	X	X
CIP-004 R3.x	X	X	X	X
CIP-004 R4.x	X	X	X	X

Requirement	EACMS	CMS (+)	EACS (+)	EAG (+)
CIP-004 R5.x	X	X	X	X
CIP-005 R1.x		+	+	X (Part 1.5)
CIP-005 R2.x		+		
CIP-005 R3		+		
CIP-007 R1.1	X	X	X	X
CIP-007 R2.x	X	X	X	X
CIP-007 R3.x	X	X	X	X
CIP-007 R4.x	X	X	X	X
CIP-007 R5.x	X	X	X	X
CIP-009 R1.x	X		X	X
CIP-009 R2.1	X		X	X
CIP-009 R2.2	X		X	X
CIP-009 R2.3			+	+
CIP-009 R3.x	X		X	X
CIP-010 R1.x	X	X	X	X
CIP-010 R2.x	X	X	X	X
CIP-010 R3.1	X	X	X	X
CIP-010 R3.2		X	+	+
CIP-010 R3.3	X	X	X	X
CIP-010 R3.4	X	X	X	X
CIP-010 R3.5	X	X	X	X
CIP-011 R1.x	X	X	X	X
CIP-011 R2.x	X	X	X	X

13. Do you agree with the SDT’s assertion that the definition of EACMS is too broad and does not differentiate the capabilities and risk(s) of the systems that fall within that definition scope? If not, please provide rationale to support your position.

☐ Yes
☐ No
Comments:

14. Do you agree that the language of the proposed definitions of EACS provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

☐ Yes
☐ No
Comments:

15. Do you agree that the language of the proposed definitions of EAG provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

    ☐ Yes
    ☐ No
    Comments:

16. Do you agree that the current compliance requirements related to EACMS monitoring systems are precluding or discouraging solutions that could reduce risk to security and reliability? Please provide your rationale in support or against this assertion.

    ☐ Yes
    ☐ No
    Comments:

17. Should the security requirements for the access control portion of the EACMS to be different from the monitoring portion of the EACMS? If you do, please provide your rationale.

    ☐ Yes
    ☐ No
    Comments:

18. Should CIP-011 Requirement R2 scope be expanded to include designated storage locations for access monitoring systems? If not, please provide rationale to support your position.

    ☐ Yes
    ☐ No
    Comments:

19. Do you agree with assignment of CIP Standard requirements to each of the EACS, EAG, and CMS categories as presented in the table above? If not, please provide rationale to support your position.

    ☐ Yes
    ☐ No
    Comments:

Concept 3: Compliance Guidance

The SDT has explored the idea that no changes are necessary to the CIP Standards to address virtualization. ERO Enterprise-endorsed Compliance Guidance could be used to address many industry concerns with the proper implementation of virtualization.

20. As the standards today do not prohibit the use of virtualization technologies, do you support an approach where no changes are made to the CIP Standards in response to the virtualization issue identified by the V5 TAG? Please provide a rationale to support your position.

    ☐ Yes
    ☐ No
    Comments:

Summary

The SDT has provided very diverse concepts for your consideration. Each of these concepts can be moved forward in the drafting process independently. Please provide your responses to each of the questions below.

21. Is your organization in support of Concept 1: Modifications to allow use of secure multi-instance? Please provide rationale to support your position.

    ☐ Yes
    ☐ No
    Comments:

22. Is your organization in support of Concept 2: Modifications to the EACMS definition? Please provide rationale to support your position.

    ☐ Yes
    ☐ No
    Comments:

23. Is your organization in support of Concept 3: Compliance Guidance? Please provide rationale to support your position.

    ☐ Yes
    ☐ No
    Comments:

24. If you have additional comments that you have not provided in response to the questions above, please provide them here.

    Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

2016-02 Modifications to CIP Standards

Informal Comment Period Open through November 2, 2017

Now Available

An informal comment period is open through **8 p.m. Eastern, Thursday, November 2, 2017**, for stakeholders to provide feedback on the **Standard Drafting Team's (SDT's) approach to addressing the use of virtualization in the CIP environment**.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience any difficulties navigating the SBS, contact Wendy Muller. An unofficial Word versions of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The drafting team will review all responses received and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact, Katherine Street at (404) 446-9702 or Mat Bunch at (404) 446-9785.

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Concepts for Virtualization and Definitions
Comment Period Start Date:	10/6/2017
Comment Period End Date:	11/2/2017
Associated Ballots:	

There were 48 sets of responses, including comments from approximately 141 different people from approximately 94 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree that the proposed change to the Cyber Asset definition makes it inclusive of both physical and virtual devices, including treatment of each virtual machine and hypervisor? If you do not agree, please provide rationale to support your position.

2. Do you agree that the term programmable in the Cyber Asset definition does not need further clarification at this time? If yes, please provide rationale to support your position.

3. If programmable does need further clarification, how would you prefer it to be addressed? Use comments to detail necessary definition changes or guidance that could be developed.

4. Do you agree with the proposed definition of Centralized Management Systems (CMS)? If not, please provide rationale to support your position.

5. Do you agree that the proposed definition of ESZ more adequately applies to proper isolation of multi-instance environments, regardless of OSI layer? If not, please provide a rationale to support your position.

6. Do you agree that the proposed definition of ESZ would aid the development of future CIP Standards by providing a more relevant level of separation? If not, please provide a rationale to support your position.

7. Do you agree that the proposed CIP-005 Requirement R1, Part 1.6 provides sufficient security controls for the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS to reduce the stated risks inherent to virtualization? If not, please provide a rationale to support your position.

8. Do you agree that the proposed CIP-005 Requirement R1, Part 1.7 provides a necessary security control to the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s) to reduce risks inherent to virtualization? If not, please provide a rationale to support your position.

9. Do you agree that the proposed CIP-005 Requirement R1, Part 1.8 provides sufficient security control to reduce the risks associated with shared multi-instance environments? If not, please provide a rationale to support your position.

10. The SDT asserts that the proposed CIP-005 Requirement 1, Part 3.1 provides additional security controls for remote access when performing CMS functions. These are necessary to reduce the risk associated with remote access to multi-instance environments. Do you agree with this assertion? If not, please provide a rationale to support your position.

11. Should the gap between Interactive Remote Access and system-to-system communication that was exposed by the examination of the risks inherent to virtualization be addressed for systems other than high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS? If not, please provide a rationale to support your position.

12. The SDT asserts that the new proposed CIP-004 Requirement R4, Part 4.5, provides additional security control to the electronic and unescorted physical access to multi-instance environment processes which reduces the “too much privilege” risk inherent to virtualization which has been identified. Do you agree with this assertion? If not, please provide a rationale to support your position.

13. Do you agree with the SDT’s assertion that the definition of EACMS is too broad and does not differentiate the capabilities and risk(s) of the systems that fall within that definition scope? If not, please provide rationale to support your position.

14. Do you agree that the language of the proposed definitions of EACS provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

15. Do you agree that the language of the proposed definitions of EAG provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

16. Do you agree that the current compliance requirements related to EACMS monitoring systems are precluding or discouraging solutions that could reduce risk to security and reliability? Please provide your rationale in support or against this assertion.

17. Should the security requirements for the access control portion of the EACMS to be different from the monitoring portion of the EACMS? If you do, please provide your rationale.

18. Should CIP-011 Requirement R2 scope be expanded to include designated storage locations for access monitoring systems? If not, please provide rationale to support your position.

19. Do you agree with assignment of CIP Standard requirements to each of the EACS, EAG, and CMS categories as presented in the table above? If not, please provide rationale to support your position.

20. As the standards today do not prohibit the use of virtualization technologies, do you support an approach where no changes are made to the CIP Standards in response to the virtualization issue identified by the V5 TAG? Please provide a rationale to support your position.

21. Is your organization in support of Concept 1: Modifications to allow use of secure multi-instance? Please provide rationale to support your position.

22. Is your organization in support of Concept 2: Modifications to the EACMS definition? Please provide rationale to support your position.

23. Is your organization in support of Concept 3: Compliance Guidance? Please provide rationale to support your position.

24. If you have additional comments that you have not provided in response to the questions above, please provide them here.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	1,3,4	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Southern Company - Southern Company Services, Inc.	Brandon Cain	1,3,5,6	FRCC,MRO,NPCC,SERC,SPP RE,Texas RE,WECC	Southern Company	Katherine Prewitt	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company - Southern Company Generation	5	SERC
					Jennifer Sykes	Southern Company - Southern Company Generation and Energy Marketing	6	SERC
Florida Municipal Power Agency	Brandon McCormick	3,4,5,6	FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC

					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Midcontinent ISO, Inc.	David Francis	2,3	FRCC,MRO,NPCC,RF,SERC,SPP RE,Texas RE,WECC	SRC + SWG	Gregory Campoli	New York Independent System Operator	2	NPCC

					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Terry BIlke	Midcontinent ISO, Inc.	2	RF
					Elizabeth Axson	Electric Reliability Council of Texas, Inc.	2,3	Texas RE
					Ben Li	IESO	1	MRO
					Drew Bonser	SWG	NA - Not Applicable	NA - Not Applicable
					Darrem Lamb	CAISO	2	WECC
					Matt Goldberg	ISONE	2	NPCC
Public Utility District No. 1 of Chelan County	Janis Weddle	1,3,5,6		Chelan PUD	Haley Sousa	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Associated Electric Cooperative, Inc.	Mark Riley	1,3,5,6		AECI & Member G&Ts	Mark Riley	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric	5	SERC

						Cooperative, Inc.		
					Todd Bennett	Associated Electric Cooperative, Inc.	3	SERC
					Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC
					Walter Kenyon	KAMO Electric Cooperative	1	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC

Seattle City Light	Paul Haase	1,3,4,5,6	WECC	Seattle City Light	Pawel Krupa	Seattle City Light	1	WECC
					Dana Wheelock	Seattle City Light	3	WECC
					Hao Li	Seattle City Light	4	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Bud Freeman	Seattle City Light	6	WECC
					Paul Haase	Seattle City Light	1,3,4,5,6	WECC
					Ginette Lacasse	Seattle City Light	1,3,4,5,6	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no ISO-NE NYISO NextERA Con-Ed and HQ	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Laura Mcleod	NB Power	1	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC

					Quintin Lee	Eversource Energy	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Helen Lainis	IESO	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
PSEG	Sean Cavote	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	NPCC
					Karla Barton	PSEG - PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co.	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co.	1	RF
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Mike Buyce	City Utilities of Springfield	1,4	SPP RE
					Steven Keller	Southwest Power Pool Inc.	2	SPP RE
PPL - Louisville Gas and Electric Co.	Shelby Wade	3,5,6	RF,SERC	Louisville Gas and Electric Company and Kentucky Utilities Company	Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					Dan Wilson	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC

1. Do you agree that the proposed change to the Cyber Asset definition makes it inclusive of both physical and virtual devices, including treatment of each virtual machine and hypervisor? If you do not agree, please provide rationale to support your position.

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	No
Document Name	

Comment

The proposed wording in the second sentence of the revised definition may still lead to some instances of inconsistent interpretation or application of the definition. It would be preferable to specifically use both of the terms “physical” and “virtual” in the second sentence, consistent with their use in the first sentence of the definition.

Suggested language for the second sentence: “Each virtual machine and physical host is a distinct device.”

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

- OUC has identified Concerns over the proposed definition to address virtual Cyber Assets including physical/hardware as many standards/requirements do not apply to a virtual device. For example, there are no physical i/o ports so the application of port locks (CIP-007-6 R1.2) does not exist in a virtual environment.
- The SDT should address the future proofing of the definition that will apply to all types of virtualized environments including storage, servers, switches, firewalls, routers, etc.
- The definition must take into consideration a virtual machine running on a virtual machine.
- The original terms “hardware, software and data” implied a physical device, with hardware and data residing within it. Within a virtual environment, the Virtual hosts (at the physical threshold) will be comprised of “hardware, software and data” while the virtual guests will be comprised of “software and data” however they may or may not be comprised of hardware. Virtual hosts not existing at the physical threshold may or may have physical aspects.
- We suggest that a different type of Cyber System be identified within the standards to address all infrastructure required to run the BES Cyber Asset/BES Cyber System in a virtual environment. We considered that the hypervisor becomes more impactful and may need even higher level of security controls. The BES Cyber System would continue to be those BCS that perform control & operation of the BES.
- If a follow-on sentence must be included in a definition, then the definition is not sufficient.
- If the second sentence must be retained then the clarification should make it clear that a virtual machine is by definition a Cyber Asset and not just a distinct device. However Hypervisors by their unique functioning, must include additional baseline information to ensure that the “entire system” remains stable, such as configuration information related to partitioning hardware, etc. used to prevent resource starvation.
- The requirement around baseline information is different between virtual hosts (infrastructure) and virtual guest/physical guests (BES Cyber Assets/Systems). With virtual hosts configuration information is critical and must be monitored to ensure that risks specific to virtual environments such as resource starvation are not modified without knowledge.

Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
The criteria or additional clarification for ”programmable” should be detailed in this definition.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
The interchanged use of the word Virtual Machine vs. Virtual Device can be misleading. The definition should be consistent for clarity.	

Cyber Asset:

A programmable electronic physical device or virtual machine, including the hardware, software, and data in the device or asset. Each physical host and each virtual machine are considered distinct Cyber Assets.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (“CenterPoint Energy”) does not agree with the proposed change to the Cyber Asset definition. The current definition covers virtual machines. Additionally, using the term “virtual device” without a corresponding definition may unintentionally broaden the scope of applicability. For example, it is not clear whether a container would be considered a “virtual device” alongside a virtual machine or a virtual local area network.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

We agree with the comments submitted by the APPA.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment	
N&ST supports the intent of the proposed change but believes the revised definition needs more clarity, particularly with regard to the word, “host.” Suggested wording: ”A programmable electronic physical or virtual device, including the hardware, software, and data in the device. Each virtual device, commonly referred to as a virtual machine, and the underlying hardware and operating system that serve as the host for one or more such virtual machines are to be considered distinct Cyber Assets."	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	No
Document Name	
Comment	
Request clarification on the term ”host” and how it relates to hypervisor. Consider removing this last sentence (Each virtual machine and host is a distinct device.) and move into the guidance.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	

Comment

APPA does not agree that the proposed change is inclusive and believes that there is a better way to include both physical and virtual devices. Therefore, public power proposes the following:

“Programmable electronic devices, including the hardware, software, and data in those devices.
Virtualized systems or devices are distinct devices.”

This proposed change would help in “future-proofing” the definition.

Likes 0

Dislikes 0

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

The SWG offers the following comments.

- The original definition does not exclude the use of virtualization, therefore it should be read to be inclusive of virtual systems. This is supported by the ***Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*** published in 2010. It states that Cyber Assets to be considered under CIP-002-1 include, at a minimum, “hardware platforms running virtual machines or virtual storage”.
- The addition of “physical or virtual” does not add clarity to the definition.
- The question uses the term “hypervisor”, but the definition uses “host”. Please ensure consistency of the terms. Hypervisor is the more commonly understood term.
- If the SDT is determined to revise the definition in this manner, we recommend “Each virtual machine and each host is a distinct and separate device” to provide more clarity about the treatment of each guest and host.
- ERO-endorsed implementation guidance would be a more appropriate means to address the treatment of the hardware, software, and data and provide examples of implementation.
- Virtual system cannot be categorized as “electronic” due to the fact that they have no measureable electronic output. Virtual systems simply mimic an electronic device.

Likes 0

Dislikes 0

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

The interchanged use of the word Virtual Machine vs. Virtual Device can be misleading. The definition should be consistent for clarity.

Cyber Asset: A programmable electronic physical device or virtual machine, including the hardware, software, and data in the device or asset. Each physical host and each virtual machine are considered distinct Cyber Assets.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

In a VDI environment, there may be no persistent virtual device; in some cases, only an image may exist that is then spun up at the point in time it is needed. Given the definition above, all programmable electronic devices consisting of a virtualized host would be classified as a Cyber Asset, regardless of the persistence of a virtual machine on the host that may or may not be used in the context of Applicable System. The asset hosting the virtualized host would be, itself, a completely separate Cyber Asset. Consider changing this part of the proposed definition “Each virtual machine and host is a distinct device.” to read “Each virtual device is distinct from it’s host(ing) device.”

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT signs on to the SRC comments and provides the following additional descriptive detail on the SRC’s comments, as well as responses for Questions #18 and #20.

ERCOT does not see the value of modifying the definition of Cyber Asset as noted in the comment form. The addition of the words “physical or virtual” does not add clarity to the definition. Virtual systems cannot be categorized as “electronic” due to the fact that they have no measureable electronic output. Virtual systems simply mimic an electronic device. ERCOT also notes that the current approved definition does not exclude the use of virtualization, therefore it should be read to be inclusive of virtual systems. This is supported by the ***Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*** published in 2010. It states that Cyber Assets to be considered under CIP-002-1 include, at a minimum, "hardware platforms running virtual machines or virtual storage".

In lieu of modifications to the definition of Cyber Asset, ERCOT recommends ERO-endorsed implementation guidance as a more appropriate means to address the treatment of the hardware, software, and data comprising a virtual Cyber Assets. ERCOT recommends drafting of examples of implementation through such guidance. Examples will aid industry in understanding the ways that virtual technologies can be implemented in a complaint manner.

Although we do not support modifications to the definition, if the SDT is determined to revise the definition in this manner ERCOT requests that the SDT ensure consistency of the terms. The question uses the term "hypervisor", but the definition uses "host". Hypervisor is the more commonly understood term, rather than host. We recommend the language be modified as, "Each virtual machine and each host is a distinct and separate device" to provide more clarity about the treatment of each guest and host.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends the proposed definition of Cyber Asset be changed:

from: A programmable electronic physical or virtual device, including the hardware, software, and data in the device

to: A microprocessor-based device, including the hardware and software in the device, that is programmable by the end user or contains firmware/BIOS that is updatable by the end user in the field.

Inclusions:

1. Devices that can be "flash" updated by end user personnel, such as programmable logic controllers, distributed control system controllers, and other similar devices.
2. Virtual Machines
3. Workstations
4. Servers

Reclamation also recommends adding the following terms to the NERC Glossary of Terms:

Virtual Machine (VM) – An operating system (OS) or application environment that is installed on software, which imitates dedicated hardware. Each Virtual Machine is a distinct Cyber Asset on the Host Machine.

Host Machine – A physical Cyber Asset used to run one or more Virtual Machines.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

The proposed Cyber Asset definition:

Adds Implementation and Compliance Complexity. The following terms, incorporated into the definition, are ambiguous and will necessitate creating additional glossary terms:

- virtual device,
- virtual machine, and
- virtual host.

Creates uncertainty that increases the opportunity for unintended negative consequences. For example, it is unclear if the proposed network virtualization definition establishes a scenario where VLAN on a switch becomes its own virtual device.

If the SDT concludes action is necessary, please consider the following:

A programmable electronic physical or virtual devices, including the hardware, software, and data in those devices. Each virtual machine and host is a distinct device.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

- TEC has identified concerns over the proposed definition to address virtual Cyber Assets including physical/hardware as many standards/requirements do not apply to a virtual device. For example, there are no physical i/o ports so the application of port locks (CIP-007-6 R1.2) does not exist in a virtual environment. The definition must take into consideration a virtual machine running on a virtual machine.
- The original terms "hardware, software and data" implied a physical device, with hardware and data residing within it. Within a virtual environment, the Virtual hosts (at the physical threshold) will be comprised of "hardware, software and data" while the virtual guests will be comprised of "software and data" however they may or may not be comprised of hardware. Virtual hosts not existing at the physical threshold may or may have physical aspects.
- If a follow-on sentence must be included in a definition, then the definition is not sufficient.
- If the second sentence must be retained then the clarification should make it clear that a virtual machine is by definition a Cyber Asset and not just a distinct device. However Hypervisors by their unique functioning, must include additional baseline information to ensure that the "entire system" remains stable, such as configuration information related to partitioning hardware, etc. used to prevent resource starvation.
- The SDT should address the future proofing of the definition that will apply to all types of virtualized environments including storage, servers, switches, firewalls, routers, etc.
- We suggest that a different type of Cyber System be identified within the standards to address all infrastructure required to run the BES Cyber Asset/BES Cyber System in a virtual environment. We considered that the hypervisor becomes more impactful and may need even higher level of security controls. The BES Cyber System would continue to be those BCS that perform control & operation of the BES.
- The requirement around baseline information is different between virtual hosts (infrastructure) and virtual guest/physical guests (BES Cyber Assets/Systems). With virtual hosts configuration information is critical and must be monitored to ensure that risks specific to virtual environments such as resource starvation are not modified without knowledge.

Likes 0	
Dislikes 0	

Response

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

Seattle City Light appreciates the efforts of the SDT to tackle this difficult question, and agrees with concept of the change. However, City Light is concerned about details fo the definition. As such, City Light support APPA's comments about the proposed new Cyber Asset definition.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	
Comment	
Definition does not use appropriate terminology such as host and guest. Consider addressing each virtual machine as a distinct asset instead of a ‘device’.	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	No
Document Name	
Comment	
The current definition already addresses both virtual and physical assets.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment

Yes, the proposed change to the Cyber Asset definition makes it inclusive of both physical and virtual “devices,” but the proposed change introduces new problems for compliance.

One use of virtualization that has been observed in the field is in the area of virtual desktops for Control Center operator consoles. In the observed case, a “base image” is instantiated each time a user logs in, thus giving each user a fresh system for each shift. The base image is kept up to date as required by CIP-007-6, etc. Because the Cyber Asset is considered to be the physical device on which the virtualization software runs, the changes effected by each new instance of the base image are simply data changes that are logged by log in/log out monitoring. If each new instance is required to be treated as a new Cyber Asset, per the proposed definition, then each individual instance must be documented with baselines (CIP-010-2 R1), an active vulnerability assessment (CIP-010-2 R3 Part 3.3), etc. This will prove unworkable.

The present definition permits wide flexibility in the use of virtualization technologies for BES Cyber Systems, EACMS, and PACS, as long as each VM is protected at the same level as the hardware device it is capable of running on.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

Cowlitz PUD agrees the proposed Cyber Asset definition will be inclusive. However, it may be over inclusive of devices that are not vulnerable to “network or internet” remote access. We believe the generic definition of “cyber” currently identifies computer based electronic devices that execute program instructions (code) from a memory medium, of which is living in an environment that allows modification via code execution. Electronic devices requiring physical manipulation, such as contact connections or replacement of hardware, to modify or replacement for upgrade should be excluded as they are not subject to circular code on code modification. The term “programmable electronic device” is subject to future definitional changes, and results in uncertain compliance interpretations. In agreement with APPA’s comment, we believe the definition of Cyber Asset should be restricted to a distinct virtual ***entity*** or physical device.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

TVA requests the SDT consider removing the sentence “Each virtual machine and host is a distinct device.” The term “virtual machine” carries significant connotations and potential for confusion. For example, a virtualized network switch may not be called a virtual machine, it may be a virtual router instance, virtual firewall instance, or a virtual device context. Each are somewhat analogous to the term virtual machine. However, calling out virtual machine specifically may hinder understanding.

Likes 0

Dislikes 0

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

BPA agrees that the proposed change to the Cyber Asset definition makes it inclusive of physical and virtual devices. However, the term *programmable electronic device* is NERC specific and not relevant to Cyber Security definitions in broader industry. Continued use of the term is unnecessary.

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	Yes
Document Name	

Comment

The SPP Standards Review Group would suggest that the drafting team provides clarity on the term “host” that’s associated with the proposed definition. At this point, there is some confusion about the applicability on how the term could be used.

Question:

If a registered entity has a server farm, how would a host be defined in that particular situation?

Likes 0

Dislikes 0

Response

Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP believes the proposed definition provides an applicability umbrella that enables responsible entities to scope their obligations effectively. But request that if “host” and “hypervisor” are synonymous terms, that a clarification be added to the definition or compliance guidance.	
Likes 0	
Dislikes 0	
Response	

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy agrees, assuming that "host" is equal to "hypervisor." We also have a general request that terms are used consistently throughout the requirements, definitions, and rationale/guidance. The definition of "Cyber Asset" should clarify what is meant by "host" - the question refers to "virtual machine and hypervisor" but the definition refers to "virtual machine and host." The second sentence of the definition should be clarified as to whether the virtual machine and hypervisor are different entities. Unless these updates are aimed specifically for hypervisors, we suggest avoiding using that specific terminology and instead suggest to use a more generic reference like "mulit-instance OS."	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
“Host” is inherently obvious: It supports one or more virtualized components. “Hypervisor” is the ambiguous, implementation specific term that should not be used. Suggest that use of the term “hypervisor” be entirely avoided.	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE would like to clarify that the virtual machine and host are one Cyber Asset as the virtual machine cannot operate without the host machine. This shared relationship means that neither can be separate Cyber Assets. For example, if a virtual machine has been identified as a BES Cyber Asset (BCA); the host machine that runs the virtual machine is also a BCA; which also applies to PACS, EACMS, and PCAs. Texas RE is concerned that treating the virtual machine and its host as separate Cyber Assets can cause mixed-trust virtual environments; the host runs CIP and corporate virtual machines. CIP controls are only being applied to the CIP virtual machine and not its host; even though the host "*if rendered unavailable, degraded, or misused*" can impact the CIP and corporate virtual machines.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	
Document Name	
Comment	

No consensus Request clarification on the term ”host” and how it relates to hypervisor. Consider removing this last sentence (Each virtual machine and host is a distinct device.) and move into the guidance	
Likes 0	
Dislikes 0	
Response	

2. Do you agree that the term programmable in the Cyber Asset definition does not need further clarification at this time? If yes, please provide rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light believes programmable should be clarified to clearly differentiate between configurable hardware (which was not envisioned to be in scope in the original CIP v5 or in the never-published NERC guidance, and should be in scope now) and devices that execute easily modified instructions. The risks presented by configurable hardware are much less than those from truly programmable devices, and they should not be lumped together.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

- Since it is the configuration of the Virtual Hosts software that implements many of the security controls that will be implemented in a virtual environment, for Virtual Hosts it is more important to identify the configuration as opposed to the programmability as the defining criteria.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends that any clarification of the term programmable be contained within the definition of Cyber Asset. Refer to the recommended definition of Cyber Asset in the response to Question 1.

Likes 0	

Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

Comments: As noted in question 1, ERCOT does not support modifying the definition of Cyber Asset unless a modification to address “programmable” provides clarity to address risk and aids in cyber asset identification across all entities. There is a risk of inconsistency of definition across the industry if the term is not defined. If there is not an ERO-wide benefit, it should remain up to the entity to define the term for their own purposes.

Implementation guidance should not be used to define a term. It is an illustration of a way to comply. This is fundamentally different from the authoritative purpose of a definition. Implementation guidance should not be used to define the scope of the assets as a foundation of a standard.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Comments: While we believe we know what a programmable device is in the sense of those devices that could be modified with malware, or which should have change control around upgrade processes, we still wouldn't mind greater clarity to assure there is no misinterpretation as to what is in scope for compliance.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

The definition of the word programmable means a device is capable of being programed via electronic code or configuration changes. A dip switch should not consider an electronic programmable device since a physical action is required to change the setting. However, there may be critical devices/equipment that are considered Non-programmable but can have an adverse effect on the a BES Cyber System (i.e. Net Gear –Non-managed Switches, or similar).

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE recommends clarifying the definition by adding a description for programmable: “*A programmable (able to be provided with coded instructions) electronic device (physical or virtual), including the hardware, software, and data in those devices*.”

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

- Programmable should be defined if it provides clarity of risk and aids in cyber asset identification across all entities. It not, it can be up to the entity to define it for their own purposes. There is a risk of inconsistency of definition across the industry if the term is not defined.
- Implementation guidance should not be used to define a term. It is an illustration of a way to comply. This is fundamentally different from the authoritative purpose of a definition. Implementation guidance should not be used to define the scope of the assets as a foundation of a standard.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy requests clarification as to what “data” should be evaluated. The drafting team should consider inserting the term “configuration” in front of the word “data” which we feel would clear up some ambiguity.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
TVA requests additional clarity for the term “programmable”; The ERO Enterprise-endorsed guidance does not sufficiently resolve issues with the term programmable.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	

Answer	No
Document Name	
Comment	
The lack of a definition can lead to either over or under classification of devices. It is currently up to the entity to decide. Auditors may have a different definition which can lead to a violation and devices unprotected for a period of time. Lack of a NERC definition can lead to inconsistencies between Regional Entities.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
The definition of the word programmable means a device is capable of being programed via electronic code or configuration changes. A dip switch should not consider an electronic programmable device since a physical action is required to change the setting. However, there may be critical devices/equipment that are considered Non-programmable but can have an adverse effect on the a BES Cyber System (i.e. Net Gear –Non-managed Switches, or similar)	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
Need to differentiate physical configurability, from electronically programmable.	
Likes 0	
Dislikes 0	
Response	

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
There is still a gray area where it is questionable on whether a device is programmable or not. Most would agree a device that is configured by DIP switches is not programmable. But functionally, a device that takes settings via software, but has no field-changeable executable code is no different, and it is unclear if such a device would be considered “programmable”. Another area of question would be live OS virtual machines. These devices are read-only and the executable code cannot be altered.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Given that currently most responsible entities have their own interpretation about programmable, pleased detail what "programmable" means in the Cyber Asset definition.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
• There are concerns that without definition of programmable, the scope of standards may be expanded to devices that do not meet the qualifications of BES Cyber Assets. • Since it is the configuration of the Virtual Hosts software that implements many of the security controls that will be implemented in a virtual environment, for Virtual Hosts it is more important to identify the configuration "configurable" as opposed to the programmability as the defining criteria.	
Likes 0	
Dislikes 0	

Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	No
Document Name	
Comment	
There are a few varying interpretations of the term programmable being used by the industry. Even the referenced ERO Enterprise-endorsed Implementation Guidance which is a Lessons Learned document, indicates that different Entities were interpreting the term differently. Also, the ERO Enterprise-endorsed Implementation Guidance, as the reference suggests, is meant as guidance, and not meant to be the only way to be compliant. In addition, Entities who fail to document their own definition of programmable in their BES Cyber System Categorization process or methodology, and even Entities who do document their own definition of programmable, are subject to auditor interpretation of the term, which can be different than the Entity's interpretation.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
Does "programmable" mean the ability to run custom code and the ability to make pre-defined configuration changes? Or does the ability to make configuration changes only fit the meaning of "programmable"? Please provide language clarifying electronically programmable language (e.g. not changes via dip switches).	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
The term “programmable” in the Cyber Asset definition does not need further clarification. The ERO endorsed Implementation Guidance clarifies the intent by explaining the various capability attributes that should be used to determine programmability.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP believes the current definition and the proposed definition allow entities to define “Programmable” for their context. It provides flexibility for asset identification.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
Some entities have built their own definition of “programmable” into their compliance program. A NERC term that varies from their definition could have significant impact on their compliance program. Since this is a hypothetical scenario, it is impossible to know if the impact would be to add or remove BES CA’s. Therefore, it is also impossible to know if this would negatively or positively impact cyber security.	
Likes 0	
Dislikes 0	
Response	

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer	Yes
Document Name	

Comment

ATC agrees that the term programmable in the Cyber Asset definition does not need further clarification at this time based on the following rationale. ATC closely monitored the SDT's prior attempts to define and provide guidance on this term. In addition, during earlier revisions to the standards, the SDT's formal responses to previous comments about this term have provided ATC adequate visibility into, and understanding of, the SDT's intent for the term. ATC had leveraged available information and guidance to formulate a methodology that assures programmable devices are considered for evaluation, and we have been able to provide clarity within our implementation through the use of our internally defined the term(s) Electronically Programmable and Mechanically Configurable. This approach provides our Subject Matter Experts with a uniform understanding of the term programmable that is consistent with the SDT's intent for the term thereby obviating the need for the SDT to further clarify it within the regulation.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern agrees, given the ERO Enterprise-endorsed Implementation Guidance that exists on the term "programmable", that the flexibility currently given Responsible Entities to internally evaluate and defend asset capabilities against the defined term provides adequate clarification at this time.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	Yes
Document Name	

Comment

While there can still be some confusion on the term programmable, the guidance document provides the needed information.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that the term programmable in the Cyber Asset definition does not need further clarification at this time. AZPS supports the revision of the definition to specifically address physical and virtual devices.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Some entities have built their own definition of "programmable" into their compliance program. A NERC term that varies from their definition could have significant impact on their compliance program. Since this is a hypothetical scenario, it is impossible to know if the impact would be to add or remove BES CA's. Therefore, it is also impossible to know if this would negatively or positively impact cyber security.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

There is existing guidance on the term programmable; therefore, there is no further need to clarify the term at this time.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
The definition of “programmable electronic device” by the examples in the BES Cyber Assets Lessons Learned document is sufficient to mitigate most of the risk posed by the devices in question. Additional fine-tuning of devices not identified as BES Cyber Assets can be accomplished on a case-by-case basis by audit teams in the field.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	

Answer	
Document Name	

Comment
The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

3. If programmable does need further clarification, how would you prefer it to be addressed? Use comments to detail necessary definition changes or guidance that could be developed.

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer

Document Name

Comment

Definition in Glossary. Distinction between providing parameters vs selecting pre-configured options - clarification between programmable and configurable.

Likes 0

Dislikes 0

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer

Document Name

Comment

As there are still varying interpretations of the term programmable, and the ERO Enterprise-endorsed Implementation Guidance is simply meant as guidance and not the only way to be compliant, there should be a NERC defined glossary term established and industry accepted definition for programmable

Likes 0

Dislikes 0

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer

Document Name

Comment

I would suggest that a separate definition is created to address infrastructure. With Infrastructure identifying configuration as opposed to programmability as criteria. If infrastructure is associated with BES Cyber Assets and could impact the BES Cyber Asset 15minute test then it must be identified and protected.

Likes 0

Dislikes 0

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer

Document Name

Comment

We suggest adding the following wording in the definition:

“A programmable device means an electronic device with a microprocessor-based circuit board, and an operating system or firmware, where an I/O port is used for programming the device. DIP switches do not qualify as an I/O port.”

Likes 0

Dislikes 0

Response

Richard Vine - California ISO - 2

Answer

Document Name

Comment

The ISO supports the comments of the Security Working Group (SWG)

Likes 0

Dislikes 0

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer

Document Name

Comment

The term programmable needs to be removed and a more specific phrase needs to be used to clarify the boundary between non-Cyber Assets and Cyber Assets.

Likes 0

Dislikes 0

Response

Bob Case - Black Hills Corporation - 1 - WECC

Answer

Document Name

Comment

Need to differentiate physical configurability, from electronically programmable.

Likes 0

Dislikes 0

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	
Document Name	

Comment

Cowlitz PUD agrees in part with BPA that the term programmable should be retired. We differ in that the definitional objective is not clear. We believe there are four concepts requiring clear identification: A computational device or entity that:

1. Autonomously reads code assembled into a set of instructions (a program) to process data;
2. Uses a memory medium to contain the code and data using read and write actions;
3. Communicates with like or similar devices to exchange code and/or data;
4. And, installs and modifies its programs by executing a program.

Concerning "virtual devices," we believe this to be confusing. Rather, we propose BPA's use of "entity" or "virtual machine" Thus, a Cyber Asset is a “discrete device” that is contained within a physical cabinet with visible ports, or a discrete ***virtual entity or machine*** with hidden virtual ports logically contained in a "discrete device." Further, we are not confident that guidance is sufficient to convey the above in a manner that protects stakeholders from contrary audit standard requirement interpretation.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	
Document Name	

Comment

The definition should be inclusive of programmable and non-programmable in order to capture all cyber assets that can impact the BES CS’s.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	
Document Name	

Comment

We recommend a definition that the device meets all of the criteria below:

- A device that has a microprocessor and field-updateable firmware or software.
  - “Field-Updatable” would include devices that have a management port, web interface, or any external interface that would allow the introduction of a firmware, software or logic update.
  - If the device’s case is sealed in such a way that would require it to be damaged to gain access to the chipset or internal ports then the device is to be considered to be not Field-Updatable.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	
Document Name	

Comment

TVA requests the SDT clarify the intent as requested by the V5 TAG.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

BPA believes that industry understands the term programmable as described in SDT Considerations for V5 Posting: “an electronic device which can execute a sequence of instructions loaded to it through software or firmware, and configuration of an electronic device is included in programmable.” The capability of being modified exists for every independent executable entity such as virtual machines or hypervisor hosts. Associated controls to prevent unauthorized or unintended modification apply to all independent executable entities because vulnerabilities may exist in either entity and are not reduced without protecting both individually.

Likes 0	
Dislikes 0	

Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy agrees that additional clarity is needed. The guidance document referenced by the SDT above, does not provide the necessary clarity on this topic. Perhaps a guideline document specific to the concept/term programmable would be beneficial.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	
Document Name	
Comment	
Recommend that a clear definition be established similar to the following: Programmable Electronic Device (PED) – A device that has a microprocessor and firmware or updateable software, which can be altered via a management port, web interface or any other external interface. A device that does not allow its internal programing to be changed, but allows a user to change between pre-defined operational parameters is considered a configurable device and not a Programmable Electronic Device.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	
Document Name	
Comment	
The SPP Standards Review Group has a concern that the term “programmable” has not been clearly defined. From our perspective, it is unclear since there is no defined term in the NERC Glossary officially referencing “programmable”. At this point, we’re not sure if the intent is to leave the term open	

and let all entities define the term in their internal programs or there is another direction the drafting team would like to go. Either way, we would like the drafting team to provide some clarity on the intent for the term.

Likes 0	
Dislikes 0	

Response
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	
Document Name	

Comment
The context included in the reference compliance guidance would be a good starting place. Consider scoping to those devices that; (1) have a microprocessor, (2) can accept firmware, software or logic, and (3) have a physical or wireless port or a web interface that can be used to “flash” firmware

Likes 0	
Dislikes 0	

Response
Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment
Please see Texas RE’s answer to #2.

Likes 0	
Dislikes 0	

Response
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	
Document Name	

Comment

The definition should be inclusive of programmable and non-programmable in order to capture all cyber assets that can impact the BES CS's.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	
Document Name	
Comment	
Comments: A document addressing the proper use of criteria mentioned. Specifically, "factors as whether a device is merely configurable, its executable code is not field upgradable, or if its functionality can only be changed via physical DIP switches, swapping internal chips, etc."	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
As noted in question 1, ERCOT does not support modifying the definition of Cyber Asset. However, if the SDT does determine that a modification is needed, the context included in the reference compliance guidance would be a good starting place. Consider scoping to those devices that; (1) have a microprocessor, (2) can accept firmware, software or logic, and (3) have a physical or wireless port or a web interface that can be used to "flash" firmware.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	

Reclamation recommends that any clarification of the term programmable be contained within the definition of Cyber Asset. Refer to the recommended definition of Cyber Asset in the response to Question 1.

Likes 0

Dislikes 0

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

Aaron Austin - AEP - 3,5

Answer

Document Name

Comment

AEP believes no further clarification of “programmable” is needed.

Likes 0

Dislikes 0

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC

Answer

Document Name

Comment

No comments from SDG&E at this time.

Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	
Document Name	
Comment	
Not Applicable.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	
Document Name	
Comment	
TEC would suggest that a separate definition is created to address infrastructure, with Infrastructure identifying configuration as opposed to programmability as criteria. If infrastructure is associated with BES Cyber Assets and could impact the BES Cyber Asset 15 minute test then it must be identified and protected.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time	
Likes 0	

Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	
Document Name	
Comment	
see response to question 2, above	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

4. Do you agree with the proposed definition of Centralized Management Systems (CMS)? If not, please provide rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light supports the concept of identifying and defining CMS, but is concerned about the details and possible unintended consequences of the proposed definition. City Light supports APPA's comments to this question. Alternatively, if the proposed definition is prefered by the SDT, City Light recommends that it be modified to apply to virtualized systems, as follows:

CMS: A system used for administration or configuration of VIRTUALIZED BES Cyber System(s) through which the configuration of the VIRTUAL BES Cyber System(s) can be altered. (new words in CAPS; deleted 2nd word "centralized" as unnecessary)

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

The current proposed definition is too ambiguous and will pull in unintended systems and potential classification of a device as both an EACM and a CMS.

The definition as proposed should be revised to only include the administration of the BES Cyber System. The current definition may expand the scope to other tools with unintended consequences. TEC suggests that the definition of CMS needs to follow the format of other Glossary Terms by referring to the configuration of BES Cyber Assets instead of BES Cyber Systems

We envision that there will either be new requirements around CMS or adding them to other requirements/parts. Our efforts here must be to protect the right devices/systems and improve the reliable/secure operation of the BES. As indicated in question 1 above, we suggest that the shared components and shared infrastructure may need different defined terms than BES Cyber System.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

KCP&L does not support the proposed Centralized Management Systems (CMS) definition for the following reasons:

Definition is Unnecessary. Introducing a new designation for this class of devices is unnecessary.

Overly Burdensome Implementation. The company's analysis estimates it will take thousands of hours to review, update documentation with references to CMS assets, and to develop the related processes and procedures.

Alternative. If the SDT concludes the proposed definition is required to address the identified issues, an alternative approach is to modify the existing definition of EACMS to include management systems like those considered in the proposed CMS definition. The approach provides a simpler compliance view by not creating a new class of devices.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

AEP suggests that, at most, the existing definition for EACMS be modified to incorporate "CMS" functions. The CMS definition allows the benefits of (1) the CMS to be within the ESP (Transmission's current implementation) and (2) applying the CMS definition to other appropriate devices (e.g. Domain Controllers or McAfee EPO).

Likes 0	
Dislikes 0	

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer	No
Document Name	

Comment

ATC requests further consideration of the use and applicability of this term as it relates to other existing categories of Cyber Assets under purview of the Standards today, as well as those extrapolated categories of EACMS proposed later in this concept/comment form. For the below reasons, ATC does not agree with the proposed definition:

1. It is unclear if the proposed CMS definition is intentionally silent to systems used for administration or configuration of Electronic Access Control and Monitoring Systems (EACMS) or Physical Access Control Systems (PACS)? Does this infer that EACMS and PACS cannot be virtualized? Where EACMS and PACS are virtualized, is an associated CMS to be identified and protected?
2. In addition, the creation of a newly defined term increases the number of Cyber Asset classification categories, thereby creating the potential for a given Cyber Asset to have yet another categorization. Careful consideration must be given to the controls applicable to each category so as to assure they are not at odds with each other. Where a Cyber Asset's functionality results in categorization under multiple categories, an unintended consequence cannot be the impossibility of compliance due to conflicting applicable controls.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support the proposed definition of CMS. Reclamation recommends the term CMS be changed to Virtual Centralized Management System (VCMS) and the proposed definition be changed:

from: A centralized system used for administration or configuration of BES Cyber System(s) through which the configuration of the BES Cyber System can be altered.

to: A centralized system used to administer or configure virtual BES Cyber System(s) or virtual BES Cyber Asset(s).

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT notes that the definition is not limited to virtualization. This also introduces questions to some fundamental understanding of physical systems that have been in place since CIP Version 1. ERCOT does not see the value defining Centralized Management System (CMS) as noted in the comment form. It should be left to the determination of the entity on the classification of the systems. The ***Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*** published in 2010 addressed the concept of management systems. When identifying CCAs, entities were encouraged to consider Cyber Assets in a secondary or supporting role. Based on this guidance, an entity may choose to high watermark the management systems to be equivalent to what they manage due to risk. This means that a management system for a BCA could be classified as a BCA. This approach could also have been applied to EACMS devices.

However, if the SDT is determined to treat management systems as a distinct class of devices, the management systems should be added to the definition of EACMS. Splitting these out will lead to inconsistency in the application of security controls across asset types and increase risk to security programs. Adding management systems to the EACMS definition will present minimal disruption for entities based on the proposal to remove monitoring from the definition.

With regards to the CMS definition proposed, the SDT should clarify the use of "centralized" in the term. The context of "centralized" should be defined. Would this apply to distributed management tools in a virtual environment?

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company has concerns that the proposed definition too broadly scopes in system-to-system management consoles used for things like patch management, malicious code prevention signature updates, and other systems that may currently not meet any applicable system definitions that would bring them into scope of the CIP requirements. For example, SCOM/SCCM and Symantec Endpoint protection used to push security patches and AV signatures to enterprise systems, and currently classified as BCSI repositories, would be scoped in and subject to additional compliance requirements as a CMS. Additional clarification is needed to understand the full scope of systems that this proposed definition would apply to. Also, the above notes state "adequately address the risk of systems used to manage virtual environments" and initially speaks specifically to "management systems in a virtual environment", yet, the proposed definition would be applicable to all environments, physical or virtual. The currently proposed definition could have further reaching impacts to management systems that are not used in virtual environments, and is overly broad and does not properly scope to virtualized environments.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Comments: So many systems if used incorrectly or maliciously can gravely affect multiple cyber assets in a BES Cyber System. These include centralized antivirus systems where a defective signature file (e.g. McAfee) could shutdown systems, centralized patching systems, baselining systems (e.g. Tripwire), vulnerability detection systems (e.g. Nessus), software defined networking systems and others. To single out virtualization control consoles seems short-sighted as it does not relate directly to the virtualized devices once they are provisions. There are also the issues around whether a client computer with a fat-client application for VM provisioning is particularly more of a risk, than a system that has a web-interface to the hypervisor that can also effect provision. In summary, centralized control systems are their own security domain, and should either be addressed separately, or under the auspices of protections afforded to all physical and virtual cyber assets.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

While we agree that the appropriate option is to create a new definition, we are concerned that the proposed definition will cause confusion on the scope of the intended systems. The definition should clearly state that it applies only to mixed-mode virtual environments.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

- It should be left to the determination of the entity on the classification of the systems. The ***Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets*** published in 2010 addressed the concept of management systems. When identifying CCAs, entities were encouraged to consider Cyber Assets in a secondary or supporting role. Based on this guidance, an entity may choose to high watermark the management systems to be equivalent to what they manage due to risk. This means that a management system for a BCA could be classified as a BCA. This approach could also have been applied to EACMS devices.

- If the SDT is determined to treat management systems as a distinct class of devices, the management systems should be added to the definition of EACMS. Splitting these out will lead to inconsistency in the application of security controls across asset types and increase risk to security programs.

- The definition is not limited to virtualization. This also introduces questions to some fundamental understanding of physical systems.
- The SDT should clarify the use of “centralized” in the term. Centralized in what manner? What about distributed management tools in a virtual environment?
- Management systems could be added to the EACMS definition. This will work with minimal disruption for entities based on the proposal to remove monitoring from the definition.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE

Answer	No
Document Name	

Comment

Xcel Energy believes that further clarification of what the CMS definition refers to and the differences between EACMS vs CMS systems should be included. For example, would the term CMS be limited to virtual environments or could a malware management console also be considered a CMS?

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group has a concern that the proposed definition may have more impact on other processes besides Virtualization. We feel that if the drafting team has an intent to include other processes that they clearly state that in the proposed definition and supporting language or develop some form of rationale to explain their position on the topic.

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation

Answer	No

Document Name	
Comment	
CMS communication is usually classified as system to system communication and not interactive remote access. The intent is to clarify how entities should implement virtual infrastructure. This definition should be limited to CMS systems that support virtual systems as that is the risk being addressed. This broad of an addition would require a re-write of interactive remote access vs. system to system communication requirements.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
The proposed definition appears to apply in a much broader sense than just Virtualization management. As currently proposed, this definition of CMS could apply to non-Virtualization tools such as Patching, or Password management. This definition would broaden the scope much farther than just applying to Virtualization.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No

Document Name	
Comment	
The proposed definition of Centralized Management Systems is vague as to what is considered a “centralized system,” which could lead to ambiguity and confusion. As currently proposed, AZPS is unsure if the term is referencing hardware, software, firmware, a combination of these, or something else. AZPS respectfully submits for the SDT’s consideration a revised definition of Centralized Management System (CMS). **Centralized Management System (CMS):** *Cyber Asset(s) through which the virtualization of BES Cyber Systems and their associated EACMS, PCAs, and PACs are administered.*	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
Public power agrees with the concept of separating the management plane from the data plane. However, the current definition includes Active Directory servers and makes it difficult to maintain systems that are inside the ESP.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes the proposed definition falls well short of SDT’s intent and, if adopted, would result in endless arguments over its applicability. What does “centralized” mean? Would it apply to the administration and configuration of ALL BES Cyber Systems? Would it apply to ANY device through which an IT or OT administrator could make ANY type of configuration change? Would it apply to systems used to push software patches and/or anti-virus signature files to BES Cyber Systems (N&ST believes some Regional Entity auditors would probably assert that it does)? If it is the SDT’s intent to address systems used to create, configure, modify, and delete virtual machines, then this definition should say so explicitly. In fact, N&ST believes the SDT should consider using the well-understood term, “hypervisor” in any proposed definition.	

Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy disagrees with the proposed definition of Centralized Management Systems (CMS) due to the potential for mis-interpretation of the word “centralized.” Entities may avoid classifying management systems as CMS because they are not centralized or, in the case of a PC running a management tool, because they are not “systems”. Vendors provide centralized management systems that automate management of many systems, but the proposed definition could apply to any system that manages another, even if there is only a one-to-one relationship and even if the management is performed by an administrator running commands or simple scripts from a terminal. CenterPoint Energy believes both scenarios do not meet the intended definition of “Centralized Management System,” but the proposed definition may create uncertainty as to the applicability. Further, many management consoles are embedded systems incapable of the security controls required by the standards. Finally, it seems the intent of the SDT is to classify hypervisors as a CMS, but the hypervisor is local, not centralized, and can only impact guests running on that machine. The CMS concept is better left to the entity to categorize, based on impact of unavailability, degradation, or misuse of the management systems on BES reliability.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx

Comment

Please see attached comments

Likes 0

Dislikes 0

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

The definition as presented is overly broad and would pull in many other types of systems in place for other functions. Systems such as centralized backup, patching platforms, or anti-malware policy servers are certainly capable of modifying the configuration of an Applicable System, but are not currently in scope. They would be unnecessarily brought into scope by this definition. It should be made clear in the definition that CMS would only apply to virtual/multi-instance configurations.

Likes 0

Dislikes 0

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Any management system that can alter the configuration of BCS should be included rather than only the centralized management system, whereas the CMS definition excludes the decentralized management system. Moreover, it can cause dual classification issue as some CMS devices could be the EACMS. We disagree to creating unnecessary new terms that are used to cover the management system and differentiate the electronic access control from the electronic access monitoring devices. These new terms can cause more confusing and more work for the entities to reclassify EACMS and identify the CMS while EACMS have complied with CIP standards. Furthermore, this would require SDT to update all applicable Systems in the CIP standards and create additional requirements for the newly reclassified and identified Cyber Assets such as CMS, EACS and EAG. To meet the same goal and reduce the complexity, we suggest modifying the EACMS definition to include all Cyber Assets that can alter the configuration of BCS into EACMS definition as follows:

“Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems and the cyber systems that can alter the configuration of BES Cyber System.”

Likes 0

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

Definitions should not rely on words from the term being defined. In this case, the use of “centralized” in the definition is unnecessary. Also, the definition contains redundant wording. Suggested wording: “One or more Cyber Assets used for administration or configuration of one or more BES Cyber Systems.” The capability for administration or configuration includes the ability to alter a configuration.

Also, this appears to be a new class of system that should be protected by the CIP Standards. Which Standards, Requirements, and Parts will need to have “CMS” added to their Applicable Systems designations?

Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	

The definition as proposed should be revised to only include the administration of the BES Cyber System. The current definition may expand the scope to other tools with unintended consequences. Does the definition of CMS need to follow the format of other Glossary Terms by referring to the configuration of BES Cyber Assets instead of BES Cyber Systems? Or is it sufficient as it stands? Does it apply to the administration only of the BCS?

We envision that there will either be new requirements around CMS or adding them to other requirements/parts. Our efforts here must be to protect the right devices/systems and improve the reliable/secure operation of the BES.

Based on group discussions, we have concerns over what is meant by administration or configuration. There were different interpretations based on individual understanding. This should be resolved with a defined term that can be plugged in to the requirements and be implemented by industry. As indicated in question 1 above, we suggest that the shared components and shared infrastructure may need different defined terms than BES Cyber System

It is becoming probablamatic when we have devices that meet multiple definitions, and potentiall when these definitions are used for determinint applicability. I can envision a device being part of a PACs and being a CMS at the same time. Is the CMS intended to be limited to just BCA's and not control devices that are implemented to meet a requirement?

Current definition is too ambiguous and will pull in unintended systems (possibly something that would be both an EACM and a CMS)

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

This is nearly complete, but still has issues. It is suggested to change this to read “A centralized system used for administration or configuration of BES Cyber System(s) through which the configuration of the managed BES Cyber System(s) can be altered or deleted when no longer needed.”

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

Is CMS intended to extend to BCSs that have no virtual components? If so, this might be outside the scope of the virtualization mandate.

To further the earlier question about if AD is intended to be included in a CMS definition, would the user, group, and permissions management functionality fall under CMS definition or would that continue to be EACMS functionality (or the new EACS category)?

Suggest that a CMS be defined as permanent to distinguish from Transient Cyber Assets used for administration/configuration. The risk associated with a CMS would be greater because it could be used inappropriately at any time and potentially remotely. Even if the CMS used the proposed CIP-005 R3 method of communication that might be intermittent, presumably that communication channel would be “on demand” and so would be present the same risk as a permanently connected system.

Likes 0	
Dislikes 0	

Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Without context of virtualization the definition is too broad and may include systems/assets which are not in scope; the other comment is the definition “Centralized Management System” uses the word centralized to define it, not the function.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
Does this apply to individual assets as part of a BES Cyber System, or only the BES Cyber System in aggregate? A BES Cyber System would typically have a mixture of assets under disparate CMS control.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
We agree that with the model proposed by the SDT, that the term Centralized Management System needs to be defined but are feel that the existing definition provides the clarity needed.	

By just applying the CMS definition and not including any previous conception of a CMS I have the following concerns.

1) Could a Transient Cyber Asset used to configure BCS (protection relays) be considered a CMS? It is probably not a “Centralized system” but I don’t know what that is.

2) Could the cyber systems, owned by the entity or a SCADA vendor, uses to remotely administer or configure multiple SCADA systems (possible at multiple entities) be considered a CMS? Using a intermediate system may eliminate the “centralized system” applicability but would still allow the remote computer to be a CMS in a low impact configuration that does not require an intermediate system.

3) The current definition would identify an Active Directory Server as a CMS. Is this what is intended?

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

It is BPA’s opinion that the proposed definition of CMS captures most types of systems that support automation with a large span of control and privileged access.

BPA recommends that the SDT moves away from the old model of devices and prescriptive requirements to a model of systems and security objectives. Under the current approach, Applicable Systems definitions are necessary to target requirements. However, under a security objectives-based approach, definitions of Applicable Systems would be less critical.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC

Answer	Yes
Document Name	

Comment

We agree that with the model proposed by the SDT, that the term Centralized Management System needs to be defined but are feel that the existing definition provides the clarity needed.

By just applying the CMS definition and not including any previous conception of a CMS I have the following oncerns. 1) Could a Transient Cyber Asset used to configure BCS (protection relays) be considered a CMS? It is probably not a “Centralized system” but I don’t know what that is. 2) Could the cyber systems, owned by the entity or a SCADA vendor, uses to remotely administer or configure multiple SCADA systems (possible at multiple entities) be considered a CMS? Using a intermediate system may eliminate the “centralized system” applicability but would still allow the remote computer to be a CMS in a low impact configuration that does not require an intermediate system. 3) The current definition would identify an Active Directory Server as a CMS. Is this what is intended?	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA supports the definition of CMS. Suggest consider clarifying that the CMS definition isn’t meant to be specific to physical or virtual CMS systems.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz PUD supports BPA's comment.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	

Answer	Yes
Document Name	

Comment

We agree with the definition, but it potentially includes systems outside the scope of virtualization – e.g., a network configuration management system can be used to push out configurations to various networking components, configuration management software (e.g., Puppet, Salt, Chef, etc.) can do the same for virtually any class of cyber asset. Similar systems exist for IEDs (e.g. Subnet Solutions PowerSYSTEM Center, EATON IMS, etc.) A domain controller can push out group policy, altering the configuration of a BCS.

Is the intent for these systems to be covered by this definition?

- If yes, that is the intent, then the definition is fine.

- If no, it is meant to only encompass virtualization management systems, then the definition is too broad and covers more than just virtualizion management systems as written.

Regardless, we believe that all configuration management systems that could affect BCS should be covered because they all have the potential to have impactful effects on the BCS whose configurations they manage.

Likes 0	
Dislikes 0	

Response

Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Rather than introduce a new term, Texas RE recommends the SDT consider adjusting the existing EACMS definition, which has been applied (applicable systems) to the CIP Requirements already. Texas RE inquires which parts of the requirements would include the new definition of CMS?

Likes 0

Dislikes 0

Response

Richard Vine - California ISO - 2

Answer

Document Name

Comment

The ISO supports the comments of the Security Working Group (SWG)

Likes 0

Dislikes 0

Response

5. Do you agree that the proposed definition of ESZ more adequately applies to proper isolation of multi-instance environments, regardless of OSI layer? If not, please provide a rationale to support your position.

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

Creating a new definition for the same concept of an ESP is counter-productive and does not add additional clarity. Additionally, even if we reused ESP, the definition above is not clear. Keep using ESP, but change the definition to be explicitly clear that either physical or virtual (logical is implied with the use of virtual) networks are allowed for the creation of the required security perimeter to isolate network boundaries. As example, "The logical border network border with one or more defined EAPs implemented using physical network topology or virtual (software defined) network tools to which BES Cyber Systems are connected using a routable protocol." This at least defines the allowed methods and the expected boundary without adding a new term with a vague definition.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

What will be required to have logical separation? Need a logical definition. Do ESP's become mandatory ESZ's?

Baselines for virtual devices—hypervisor, need more data than just the ports & service, OS, SW, patches (resource definitions, other security controls, to do comparison). Configuration must prevent resource starvation—hardening guide for VMware—SSH port/TFE….

What is sufficient here: "proper isolation of multi-instance environments"? Can't create a requirments that relies on entities and auditors to interpret what is proper isolation. Need to define it and or replace the language.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No

Document Name	
Comment	
The meaning of “logical separation” needs to be better defined.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
The term **area** in this context needs to be defined or clarified. We suggest rewording the definition: “The area within a networking environment with a defined logical boundary that logically separates one or more Cyber Assets.”	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
The proposed definition is not specific enough to pinpoint multi-instance environments. The definition should be limited to ensure that it only applies to virtual environments. Additionally, it should be made clear that all Cyber Assets within the ESZ should reside within the same logical network.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	

Comment

Yes, in theory. If infrastructure was shared, then ESZ would make sense. Would like to see more technical detail to the definition to know where NERC is going with this, to justify the additional term as compared to sticking with just ESP.

Likes 0

Dislikes 0

Response

Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA

Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx

Comment

Please see attached comments

Likes 0

Dislikes 0

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not agree with the proposed ESZ definition. The term “area” is ambiguous and open to interpretation. Rather than creating a new concept such as ESZ, the SDT should consider adding language to the requirements that provide logical separation between assets. Additionally, it may be challenging to document evidence that demonstrates an ESZ.

Likes 0

Dislikes 0

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

Refer to question #23 comments.

Likes 0

Dislikes 0

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer No

Document Name

Comment

N&ST considers this proposed definition, as written, to be essentially identical to the existing definition of ESP. It appears to be the SDT’s intent to apply the concept of logical separation to virtual machines running on shared hardware/software infrastructures, in which case the definition should be written so as to make this explicit.

Likes 0

Dislikes 0

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer No

Document Name

Comment

TVA supports flexibility within the standard to accommodate a multi-tenant architecture and the benefits provided by adaptation of industry standard architectures such as on premises cloud computing and hyper-converged infrastructures. TVA is concerned the ESZ concept as presented is overly complex and creates potential to hamper entities in constructing appropriate security controls or programmatic boundaries for their compliance programs. Loading definitions and program boundaries with new, undefined terms such as “multi-instance, shared infrastructure, management plane, data plane, and containers,” will only compound confusion and fragmentation of interpretation.

Likes 0

Dislikes 0

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer No

Document Name	
Comment	
AZPS believes the proposed definition does not adequately address the controls needed to perform the necessary separation. AZPS respectfully proposes a revision to the definition of Electronic Security Zone. **Electronic Security Zone:** *A segment of infrastructure services containing one or more Cyber Assets that is established using a logical border and to which the Responsible Entity has applied specific security controls.*	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA. Additionally, Tacoma Power has concerns that the boundaries of logical segmentation can be unclear with shared memory, storage and network interfaces.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
This definition is not limited to just systems using virtual technologies and would reduce clarity and industry understanding for classifying routable vs non-routable logical separations. Include a caveat limiting ESZ to multi-tenant systems.	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standards Review Group has a concern that the proposed definition may have more impact on other processes besides Virtualization. We feel that if the drafting team has an intent to include other processes that they clearly state that in the proposed definition and supporting language or develop some form of rationale to explain their position on the topic. Also, we have a concern about how the term “logical separation” will be used or the intent of the term. For example, what defines “logical separation,” and does it have physical or technological control?	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	
The ESP and ESZ definitions should be aligned within a single definition. There is no need for two definitions that address basically the same idea. Two definitions will cause confusion. Recommend: The border that provides logical separation to isolate BES Cyber Systems from other Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Comments: How appropriate various forms of logical and physical isolation are will always be dependent on the software and hardware implementations. A definition of the boundary between a VM and its hypervisor, or a VM and another VM may be useful to delineate a boundary where security/isolation controls can be evaluated/applied, but by no means addresses the concept of "proper isolation". The concept of proper isolation is a diffuse one and can broach on a multitude of shared infrastructure concerns, including SANs, power distribution systems, separation of computing instructions from data in hardware, etc. Risk can also be evaluated in the context of the systems design, or can encompass the possibility of privilege	

elevation bugs which further muddies the water. In summary, the isolation of virtual cyber assets isn't necessarily a greater concern than the isolation of physical cyber assets, with the possible exception of how a hypervisor might be treated. It is even conceivable that a VM platform could securely isolate even systems with different security contexts depending on the implementation.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

Please add to the end of the definition "of one or more Cyber Asset(s) in a virtual multi-instance environment." Without this clarification directly in the definition, rather than in the Applicable System section, there could be unintended consequences and confusion between ESZ and ESP for Cyber Assets that are not part of a virtual multi-instance environment.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

Comments: ERCOT recommends that the ESP and ESZ definitions should be aligned within a single definition. There is no need for two definitions that address basically the same idea. Creating two definitions will add to confusion and may require Entities that have implemented to CIP Version 5/6 to re-assess and re-design their configurations at substantial cost without much added benefit. The ESZ definition is broad and appears focused on a single or few use cases (based upon vendor technologies), but could have negative impact on other use cases (other vendors) beyond the intended purpose. ERCOT asserts that a single definition could be used to address network boundaries holistically and asked that the SDT consider a modification such as, "The border that provides logical separation to isolate BES Cyber Systems from other Cyber Assets."

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support the proposed definition of ESZ. The term ESZ can impact virtualized and non-virtualized systems.

Reclamation recommends the term Electronic Security Zone be changed to Virtual Electronic Security Zone (VESZ), applying only to virtualized environments, and the proposed definition be changed:

from: The area defined by the logical separation of one or more Cyber Asset(s).

to: A boundary housing one or more Virtual Machines logically separated from other BES Cyber Systems or other non-BES Cyber Systems using partitioned and isolated service set identifiers (SSIDs), virtual local area networks (VLANs), or other technologies.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

While the proposed definition does for today give a more specific method of isolation, AEP believes a more effective solution would be to, at most, modify the definition of ESP to allow for greater latitude in establishing logical segmentation of networks whether physical or virtual. AEP believes implementation of processes to meet CIP-005 R1, Parts 1.6-8 would produce sufficient evidence and meet the intent of the proposed requirements without introducing the new definition of an ESZ.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC

Answer	No
Document Name	

Comment

SDG&E considers this concept of an ESZ to be vague at best and problematic with compliance. Specifically the physical separation that may or may not be achieved in a virtual environment.

Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Scope Expansion Adds Complexity. The incorporation of the term “Cyber Asset” within the proposed Glossary Term can easily broaden the scope beyond isolation of multi-instance environments. Expanding the scope will create unnecessary implementation and compliance complexity. **Compliance Uncertainty.** The term “area” is vague and will create compliance uncertainty. We have not been able to identify additional prescriptive language or how to succinctly define the term to mitigate that uncertainty.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
The term “logical” should be more specific, up to and including relevant OSI layers. It should also be specified if the ESZ will require separation of specific assets from each other. In physical servers, the communication between devices in an ESP is not controlled and we believe the analogy should carry to virtual infrastructure. Two VMs of the same BES Cyber System could share an ESP and an ESZ, for instance.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

- The proposed definition of an ESZ is insufficient to provide guidance to industry.
- TEC has included some of the questions/discussion around the logical separation and layers for the SDT to better understand where the confusion may lie.
    - More than just OSI layer 3 connectivity; need to provide controls at the other layers, but which layers? Who makes the call?.
    - VMware: Can put virtual firewalls inside the cluster; can separate the traffic with controls in place. Which OSI layers—segment layer 2 or layer 3. Concept for ESZ is for non-layer 3.
    - If it is on the same SAN, if you have the potential to use the other hardware, then you have to protect it. Or could encrypt the device. Definition of Cyber Assets—electronic physical or virtual….would apply to the financial box in the image on p. 8.
    - What will be required to have logical separation? Need a logical definition and Virtual Cyber Asset…should not be physical plane into virtual plane.
    - Baselines for virtual devices—hypervisor, need more data than just the ports & service, OS, SW, patches (resource definitions, other security controls, to do comparison). Configuration must prevent resource starvation—hardening guide for VMware—SSH port/TFE….
    - Implement vendor hardening guide—(but that brings in new requirements related to

    Mixed trust—create vm dedicated to CIP; VM for high BES Cyber Systems… what about the EACMs—in a separate environment but not an ESP? What about PACS—now on corporate; separate VM environment for PACS. Will get to be cost prohibitive to use virtual environments if they all have to be separate. Every device on the virtual environment has to be treated according to the high water mark;

    - May apply to one instance but may not apply to others. What is sufficient here: “proper isolation of multi-instance environments,”

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Alliant Energy believes the ESZ definition does not adequately describe the environment options. We request clarification on the relationship between the ESZ and ESP in a virtual instance and whether the ESZ replaces the ESP or is conained within the ESP. Additionaly, the definition should distinguish between BCS ESZ and non-CIP ESZ.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Clarification of the need for an ESZ has not been established within the definition.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
Fundamentally disagree with the creation of a new ESZ concept. It seems to be an attempt to arrange virtual resources in a way similar to what is currently done with Cyber Assets as network nodes in an ESP. However they are not analogous, do not work that way and should not be managed that way. The ESZ concept is not a good fit and explains why most of remaining question is this section are difficult to interpret. Please see summary answer 21 for suggestion of a simpler approach. Also, use of “multi-instance”, if, as it seems to be, is meant to be analogous with the idea of “multi-tenant”, than this would seem to exclude most virtualized systems. Is this intended?	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6	
Answer	No
Document Name	
Comment	

The current definition is unclear.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	Yes
Document Name	

Comment

ESZ definition is good, but ESP definition should be removed and ESZ controls should be sufficient.

Likes 0	
Dislikes 0	

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	Yes
Document Name	

Comment

This definition is sufficiently high level that it could encompass any type of logical isolation.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

We support BPA's comment.

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes the proposed definition promotes proper isolation of multi-instance environments regardless of OSI layers. However, usefulness of ESZ is not limited to multi-instance environments. ESZ enables separating risk associated with different types of technology, layering of controls, and granular security in contrast to the outdated, simplistic, high-watermarking approach of ESP.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
We are concerned that because ESZ uses a different definition of “logic” than is used in the BCS definition, the definition used in ESZ could be applied to the BCS. Please provide clarification on the difference between an ESZ and an ESP.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	

City Light generally supports the ESZ concept but does not find it to sufficiently detailed or evaluated for integration with structure of the existing CIP Standards. As such City Light supports APPA's comments for this question 9especially as regards the varied meanings of "logical"), while generally agreeing with BPA's position.

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	

APPA is concerned that the ESZ uses a different definition of “logic” than is used in the BCS definition and believes the Standard Drafting Team (SDT) should share that concern.

Public power is concerned that the standard could lead to a misunderstanding that the definition of “logic” is the same for BCS, ESZ and the proposed CIP-005 R1.6.

Consequently, the standard needs clarification on how an ESP is not an ESZ.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE suggests the current term, Electronic Security Perimeter, is sufficient for protecting Cyber Assets. The BES Cyber System concept is a logical grouping; by definition a BES Cyber System is “***One or more BES Cyber Assets*** *logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity*.”

Likes 0	
Dislikes 0	

Response

6. Do you agree that the proposed definition of ESZ would aid the development of future CIP Standards by providing a more relevant level of separation? If not, please provide a rationale to support your position.

Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6

Answer	No
Document Name	

Comment

The proposed definition is not clear.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Clarification of the need for an ESZ has not been established within the definition. The current ESP and EAP terms are sufficient to describe the access control objective.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

NERC has clearly stated that Ethernet VLANs are not considered acceptable logical separation. If NERC will not accept VLANs as acceptable (which have been around for 15 years) there is no chance or at least there should be no chance that the ESZ would be found sufficient.

Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
We understand the intent is to ensure that VMs in shared environments have controls to keep their data separate, however as written it is ambiguous and appears to be adding security that doesn't exist for physical machines, e.g. separating individual virtual hosts in one BES Cyber System vs. allowing physical BES Cyber Assets in one BES Cyber System to communicate within an ESP.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
See our response to proposed ESZ definition, Question 5. Also, we do not see the proposed ESZ definition would apply any differently to future CIP Standards. **Request.** If the SDT concludes the proposed definition is required to address the identified issues, clarity is needed to understand the relationship between the Electronic Security Zones and the existing structure of the Electronic Security Perimeter. For example, are the terms ESZ and ESP complementary, or does implementing an ESZ eliminate the need for an ESP?	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	

A more thorough examination of the physical separation of the virtual environment must be addressed before a true ESZ can be made to be compliant. How does storage factor into the establishment of a ESZ?	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
While the proposed definition does for today give a more specific method of isolation, AEP believes a more effective solution would be to, at most, modify the definition of ESP to allow for greater latitude in establishing logical segmentation of networks whether physical or virtual. AEP believes implementation of processes to meet CIP-005 R1, Parts 1.6-8 would produce sufficient evidence and meet the intent of the proposed requirements without introducing the new definition of an ESZ.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support the proposed definition of ESZ. Reclamation recommends the proposed term Virtual Electronic Security Zone (VESZ) (described in the response to Question 5) will provide a more relevant level of separation. Reclamation also recommends changing the terms “instance” and “multi-instance” to “Virtual Instance” and “Multi-Virtual Instance” and adding them to the NERC Glossary of Terms using the SDT’s intended meanings as the definitions.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	

Answer	No
Document Name	
Comment	
See comments for question 5.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	No
Document Name	
Comment	
The definition, as proposed, does not properly scope the implementation of the term to virtual multi-instance environments, and could have broader impacts as currently stated.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Comments: The adequacy of separation is dependent upon the hardware and software of a specific implementation, and also to the evaluation of issues with such separation overtime. A definition as a placeholder for future VM isolation requirements seems to presuppose that the need of logical segregation for virtual cyber assets exceeds that of physical cyber assets.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	

Answer	No
Document Name	
Comment	
The ESP and ESZ definitions should be aligned within a single definition. There is no need for two definitions that address basically the same idea. Two definitions will cause confusion. A consistent approach to logical boundaries.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standards Review Group recommends that the drafting team provides more supporting detail in the definition.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
This definition reduces the clarity for levels of logical separation by adding a level. Increasing the number of logical separations a system may have adds to confusion within the standard and increases compliance complexity which is not desired.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No

Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
The proposed definition of ESZ appears to be overly broad. Does the drafting team intend that the definition of ESZ supersede the ESP? As currently proposed, situations could exist where a Cyber Asset would need to comply with both ESP and ESZ requirements.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS is concerned that the definition and concept as proposed could lead to ambiguity and confusion if it does not address all of the concepts and potential configurations indicated in this document and its associated diagrams. In particular, AZPS recommends that the definition needs to address the separation controls as mentioned in the rationale provided in Questions 5, 7, 8, etc. Additionally, AZPS recommends that the terms instance and multi-instance be revised to refer to tenancy as this is a more accurate representation of virtualized devices and environments. The term instance could be confused relative to whether it is referencing a segment of the virtualized environment or the assets within that environment. To alleviate that confusion, AZPS believes that use of the terms tenant and multi-tenant will more clearly delineate the cyber assets versus the environment. • Tenant: Discrete organizational environment with specific privileges or security levels, consisting of functions that consume resources from the shared infrastructure. Tenants are logically isolated, but physically interconnected. • Multi-Tenant: An environment where a shared infrastructure provides containers for more than one tenant.	

Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
APPA does not believe that the proposed definition for ESZ would provide the relevant level of separation needed. "Logical separation" is based on current technology and may not be applicable to future controls.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
TVA supports flexibility within the standard to accommodate a multi-tenant architecture and the benefits provided by adaptation of industry standard architectures such as on premises cloud computing and hyper-converged infrastructures. The ESZ concept, as presented, is overly complex, and lacks clarity to help entities how to institute separation between tenants, and shared underlying physical compute resources, whether processor (compute), storage, or transport (network).	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST believes a properly written definition of “ESZ” would aid in the development of future CIP requirements, but has checked “No” to reflect concerns about the inadequacy of the current proposed definition.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The ESZ concept is potentially confusing and will not aid in clarity for future Standards. Standards relevant to logical separation can state requirements for logical separation where appropriate. Further, business needs vary in different environments, and an entity may have valid reasons for not logically separating systems that do not introduce unacceptable security risks. Requiring an ESZ to be defined limits the flexibility an entity has to design and manage systems in their own environments.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	

Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
Do not see the benefit to entities of a separate term at this time. But if shared infrastructure is in place at an entity, then this could make sense.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
With an appropriately narrow definition (see #5 comments), we would consider the addition of ESZ to be adequate.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	

The ESZ definition is not clear and doesn’t define what Cyber Asset should reside in the ESZ. If all Cyber Asset inside a ESP, in our opinion, the ESZ is not necessary.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
NERC has clearly stated that Ethernet VLANs are not considered acceptable logical separation. If NERC will not accept VLANs as acceptable (which have been around for 15 years) there is no chance or at least there should be no chance that the ESZ would be found sufficient. We have concern that NERC will not accept (nor should they based on their current concerns over VLANs) this definition without the underlying acceptance of the vlans use for logical separation.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
As stated above, adding a new term without any definition of what is expected adds confusion. The proposed definition is similar to how PCI (Payment Card Industry) standards defined the use of virtualization and lead to the delay in properly defining a secure usage for the technology allowing virtual networks and micro-segmentation.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
City Light supprots the direction introduced by ESZ but believes additional work is necessary to clarify its implications and ensure its correct functioning with the existing CIP framework. City Light supports both the comments of APPA and BPA.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
“Logical separation” is based on current technology and may not be applicable to future controls. Suggest that it would be better to require the separation and that the separation could include logical methods but not limiting it to just logical.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	

Having another defined term for a security zone helps provide additional clarity.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

As virtualization matures in this industry, it will require a more effective construct than the existing ESP. ESZ is the more effective construct for multilayered, modern security strategies as opposed to ESP which is one dimensional and has been applied at one layer of the OSI model.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC

Answer	Yes
Document Name	

Comment

“Logical separation” is based on current technology and may not be applicable to future controls. Suggest that it would be better to require the separation and that the separation could include logical methods but not limiting it to just logical.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

We support BPA's comment, but also caution development to allow for future advances in controls.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

With a stronger definition of ESZ, this concept may be worth pursuing.

Likes 0	
Dislikes 0	

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	Yes
Document Name	

Comment

It is difficult to tell from the definition alone. It would need to be shown in context to determine if it is useful. It is sufficiently high level to cover many different types of logical separation, but it may be so abstract that entities will have trouble interpreting what to do. Based on some of the following requirements though, it looks like it will aid in development of future CIP Standards.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	

No comment at this time	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s response for #5.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

7. Do you agree that the proposed CIP-005 Requirement R1, Part 1.6 provides sufficient security controls for the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS to reduce the stated risks inherent to virtualization? If not, please provide a rationale to support your position.

Scott Downey - Peak Reliability - 1

Answer	No
Document Name	

Comment

In many instances the management plane uses centralized authentication such as radius or Idap. This makes the management plane dependent on the supporting authentication servers. The supporting authentication servers often have a managmeent backplane. For simplicity the managment plane of the authentication servers may be connected to the date plane as the benefit of separating the planes is limited due to the dependency.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

This is close, but needs more definition and a requirement to ensure that the CMS still reside within the ESP (again remove the use of an ESZ as this adds more confusion). Suggestion re-write:

Logically separate, using Hypervisor controls and an associated CMS, all Applicable Systems into defined groups of one or more Cyber Asset(s) to achieve the objective of mitigating the risks of span-of-control, insider threats, and lateral privilege expansion. At a minimum:

1. The management plane (CMS) and the data plane of the managed BES Cyber system shall be separated on different managed networks while ensuring both must reside in the same ESP.
2. The CMS of the managed BES Cyber Systems shall be separated from the data planes in which the BES Cyber Systems operate.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment	
Part 1.6.1 potentially mitigates the risk of lateral privilege expansion and possibly insider threats We are concerned that none deal with mitigation of span-of-control In addition, not all vendor solutions may be able to address Part 1.6. If it is added, there should be TFE capability. In addition, the proposed Part 1.6 introduces the requirement for lists to demonstrate compliance. We also suggest that the word "achieves " is not the appropriate term for the requirement part. We recommend changing it as follows: Logically separate all Applicable Systems (is this a new defined term?) into defined groups of one or more Cyber Asset(s) to **address potential risks** related to span-of-control, insider threats, and lateral privilege expansion.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
This concept has great promise, but terms need to be either defined in the Glossary (preferred), or explained thoroughly in a Technical Guidance document that can become Implementation Guidance. Also, consider adding EACMS and PACS to the applicable systems, as EACMS and PACS can benefit from virtualization technologies as well.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	

We suggest changing the wording from “defined groups of one or more Cyber Assets to “defined ESZs”. Also we suggest changing the wording from “The management plane and the data plane of the applicable BES Cyber System shall be separated” to “The management plane and the data plane of the applicable BES Cyber System shall be separated by ESZ”. As we proposed EACMS definition modification, “CMS” would be changed to “EACMS”. Please clarify whether the management plane and data plane need to be separated by ESZ, provided that both planes reside inside ESP. Given that the modified Cyber Asset definition includes physical and virtual devices, this requirement will apply to physical cyber system as well, where it means the current in-band network architeture is required to be changed. For instance, an EACMS inside ESP would requires a ESZ to separate it from the BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

CIP-005 R1.6 should explicitly require the defined groups to be ESZs rather than implicitly. "Logically separate all Applicable Systems into Electronic Security Zones to achieve the…”.

Additionally, “span-of-control, insider threats, and lateral privilege expansion” should be removed from the proposed requirements and moved to the Guidance and Technical Basis.

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA

Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx

Comment

Please see attached comments

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The Requirement language as written will be challenging for entities to demonstrate compliance because it is objective and intent based. Registered entities may have difficulty producing evidence of intent. Also, entities may encounter situations where there is a valid reason for not separating the management and data plane of an asset or system, and the proposed Requirement R1, Part 1.6 would not allow that. Further, many assets do not have a capability of logical separation of management and data plane. For those that do have the capability of such separation, it is not clear what evidence can be provided to prove the separation is achieved and that no management activity has or can occur from the data plane. This requirement seems to be aimed at multi-instance environments but does not state this in the language, and it would be difficult to achieve and demonstrate for many non-virtual environments. If the proposed Requirement R1, Part 1.6 is intended for multi-instance environments, the wording should be revised to make such intent clear.	
Likes 0	
Dislikes 0	
Response	

Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST considers the stated objectives to be worthy but they should not be included in a requirement statement. How would an entity actually demonstrate they have effectively mitigated the identified risks? N&ST assumes “applicable systems” are “BES Cyber Systems comprising one or more virtual machines” and “associated CMS” but the SDT should say explicitly what are “applicable systems.” N&ST wonders why the SDT, having defined “ESZ,” doesn’t use it here. Why not say, “The data and management planes of applicable systems shall reside in separate ESZs”? N&ST also	

recommends that, at a minimum, any potential requirement such as this include a brief description of what is meant by “management planes” and “data planes.”

Likes 0	
Dislikes 0	
Response	

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC

Answer	No
Document Name	
Comment	

Too prescriptive because some products do not allow separation of management and data planes

It is difficult to answer this question because it is not completely clear what the proposed R1.6 requires.

The first part of this requirement is almost identical to the definition of ESZ. If this requirement is to implement ESZ(s) than it should use the ESZ term. If not, it should be clarified on how this is not an ESZ.

Have the same concern as with the use of “logical” in the ESZ definition. The use of “logically separate” in this requirement could redefine the “logically grouped” in the BCS definition. How is “logically separate … into defined groups” used here different than “logically grouped” used in the BCS definition?

Likes 0	
Dislikes 0	
Response	

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	
Comment	

While AZPS agrees with the intent to separate the management and data plane, it suggests that the proposed CIP-005, R1.6 is not as clear and unambiguous as it could be and, therefore, could result in confusion regarding applicability. To ensure that the scope of the requirement is clear, AZPS recommends that the language of R1.6 specifically reference virtual, multi-tenant environments.

Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy requests additional clarity as to what the SDT is referring to when referencing lateral privilege expansion. Also, as written, ambiguity exists as to the actions that an entity will need to take to comply. In some instances, more actions may need to be taken to address the risks mentioned in Part 1.6.	
Likes 0	
Dislikes 0	
Response	

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standards Review Group recommends that the drafting team needs to better identify or define what the two terms “management plane” and “data plane” mean. Also, we would recommend that there be an illustration provided for Part 1.6 as it is in Part 1.8. Question: Does the drafting team intend for the management plane to always be included in the ESP as illustrated in figure 1.8 shown below?	
Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

- The SDT should clarify the meaning of separation. Is this intended to be routable protocol separation or memory separation within the hypervisor itself? Seems to be a judgment call.
- Refer to the diagram below. It shows management and data plane in the same ESP.
- Consider defining span of control and insider threats?
- Lateral relative to what?
- The security objective adds confusion.
- The requirement could simply state “Logically separate Applicable Systems”.
- What does “its” refer to in #2?
- Management and data functions should be defined and common access prohibited

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Comments: While defining groups of cyber assets (physical or virtual) that need to communicate to perform a function, and isolating/limiting such communication within the group makes sense, bringing management and data planes into the standards when so many products do not even have a cohesive mapping to the concepts seems unwise, not to mention the omission of the control plane.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company views the proposed requirement as being too prescriptive, reducing the Responsible Entities flexibility in implementing secure concepts in a virtual environment. The SDT should consider also defining the terms “management plan” and “data place” to provide better understanding and specificity.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT asserts that the requirement increases complexity while creating confusion for Entities that have already implemented CIP Version 5/6. The standard requires an Entity to configure and implement based upon specific configurations concepts creating risk for other technologies. Result or outcome-based standards should be used and not be as prescriptive as the requirement proposed. This allows Entities to use definitions to illustrate their architecture and implementation.

ERCOT offers that the requirement could simply state “Logically separate Applicable Systems”. The proposed requirement offers a security objective, but also goes into specifics that are prescriptive in nature. The SDT should ensure that a proposed requirement is clear and implementable as defined by industry.

With regards to the proposed requirement, ERCOT offers the following feedback. (1) The SDT should clarify the meaning of separation. Is this intended to be routable protocol separation or memory separation within the hypervisor itself? Seems to be a judgment call, which is not appropriate for a mandatory and enforceable requirement. (2) The SDT should consider defining span of control and insider threats. (3) ERCOT requests clarification of the context of “lateral”. Lateral relative to what? (4) The SDT should clarify what “its” refers to in item 2 of the requirement. (5) Management and data functions should be defined and common access prohibited. ERCOT also notes that in the diagram below, the management and data plane in the same ESP.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support the addition of Part 1.6. Reclamation recommends that revising the definition of BES Cyber System and the Impact Rating Criteria will provide sufficient security controls and reduce the stated risks inherent to virtualization. Refer to the principles, recommended definitions, rationale, and recommended Impact Rating Criteria described in the response to Question 24.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ATC agrees that the proposed addition of CIP-005 Requirement R1, Part 1.6 addresses span of control and lateral privilege expansion. However, ATC does not feel it sufficiently addresses insider threats. ATC suggests striking “insider threats” from the requirement as logical separation does little to stop an insider with knowledge of the environment.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	No
Document Name	
Comment	
Too prescriptive because some products do not allow separation of management and data planes It is difficult to answer this question because it is not completely clear what the proposed R1.6 requires. The first part of this requirement is almost identical to the definition of ESZ. If this requirement is to implement ESZ(s) than it should use the ESZ term. If not, it should be clarified on how this is not an ESZ.	

Have the same concern as with the use of “logical” in the ESZ definition. The use of “logically separate” in this requirement could redefine the “logically grouped” in the BCS definition. How is “logically separate … into defined groups” used here different than “logically grouped” used in the BCS definition?	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
SDG&E considers this proposed requirement to be far too undeveloped to be considered for advancement. SDG&E would like more detailed explanations of the separation of management plane, storage element and data plane. Seek further clarification of where the CMS can reside and be compliant with this requirement. How does a multi-impact criteria CMS meet this requirement?	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	

Comment	
The proposed CIP-005 R1, Part 1.6. creates: **Compliance Uncertainty.** The terms “applicable systems,” “span-of-control,” “insider threats,” and “lateral privilege expansion” used in proposed Part 1.6 can easily be construed and interpreted broadly, creating significant compliance uncertainty. Recognizing that some of the terms occasionally popup within the context of cybersecurity, we have not been able to identify additional prescriptive language or determine how to define the terms to mitigate that uncertainty. Without additional clarity, the terms create compliance uncertainty. **Burdensome Costs.** The cost to implement and maintain Part 1.6 compliance is burdensome. The compliance uncertainty associated with the subpart further muddies determination of the eventual security benefit, if any. **System Performance Impacts.** It is expected that implementing Part 1.6 will require new or modification to current systems, processes, and procedures. The added complexity will unfavorably affect system performance. **Unintended Consequence.** It is generally accepted that added complexity weakens security by increasing potential cyber vulnerability paths.	
Likes 0	
Dislikes 0	
Response	

John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
These terms appear to specifically reference VMWare NSX. The webinar showed that it would be acceptable to address management interfaces on one LAN and the public VM on another. That makes sense to us and is a best-practice in general. That said, the definitions should reflect that concept better and be specific about how “deep” that separation needs to be, e.g. does it require two ESPs? Can they be VLAN-separated? (See later comments on VLANs.)	
Likes 0	
Dislikes 0	
Response	

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

We suggest that the proposed requirement Part 1.6 could this be a policy with entity documentation of risk mitigation.

1. Part 1.6.1 potentially mitigates the risk of lateral privilege expansion and possibly insider threats
2. We are concerned that neither minimum inclusions deal with mitigation of span-of-control

In addition, not all vendor solutions may be able to address Part 1.6. If it is added, there should be TFE capability. In addition, the proposed Part 1.6 introduces the requirement for lists to demonstrate compliance. We also suggest that the word “achieves“ is not the appropriate term for the requirement part. We recommend changing it as follows:

Logically separate all Applicable Systems (is this a new defined term?) into defined groups of one or more Cyber Asset(s) to address potential risks related to span-of-control, insider threats, and lateral privilege expansion.

Likes 0	
Dislikes 0	

Response

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light supports the concept of the new requirement but cannot support the wording. Management plane and data plane must be clarified or defined, if used within a legal requirement, and the term "Cyber Asset" must be modified to ensure only 'applicable' or 'virtualized' Cyber Assets are in scope, not all possible Cyber Assets (because the CIP Standards only apply to BES Cyber Assets and applicable Cyber Assets as identified by CIP-002, and not all possible Cyber Assets). Considerable conflict remains between the logical-based concepts on ESZ and the physical-based concepts of devices and Cyber Assets.

City Light further supports APPA's additional comments.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

The new requirement may be adding complexity without addressing the security objective.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

Agree this is a good idea. However, in practice what it means is most control, at least in terms of interaction by a user through a CMS cyber asset, is via network connection. The simple approach is to require all such CMS cyber assets (virtual or real) to be in a distinct ESP from the hosted cyber assets. Possibly a requirement could be made that any non-IP interaction (a proprietary management plane or direct hooks into the host OS) b/w the CMS cyber asset and the host have some security provisions, but this is usually proprietary and vendor specific and difficult to define in a universal way.

Likes 0	
Dislikes 0	

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	Yes
Document Name	

Comment

Yes but there needs to be some provision for separating the management planes for BCA and non-BCA. Separation of the management plane is necessary to ensure Cyber Assets are appropriately categorized and that unnecessary cyber assets are not brought into scope when not needed to be.

For instance some entities will use one CMS for all virtualized Cyber Assets. Some of these may be BCA, some may not. Entities will often separate the data planes of these virtual Cyber Assets, but may forget to separate the management plane, thus inadvertently making all of the non-BCAs PCAs even though the data planes are separated. There should be some guidance on this topic to make sure entities are separating virtualized Cyber Assets appropriately.

Likes 0	
Dislikes 0	

Response

Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
: **But should only apply to CMS for BCS.**	
Likes 0	
Dislikes 0	
Response	

Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
We support BPA's comment.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA supports flexibility within the standard to accommodate a multi-tenant architecture and the benefits provided by adaptation of industry standard architectures such as on premises cloud computing and hyper-converged infrastructures. The ESZ concept, as presented, is overly complex, and lacks clarity to help entities how to institute separation between tenants, and shared underlying physical compute resources, whether processor (compute), storage, or transport (network). In the language provided, it is unclear as to the target of the separation (e.g., specific groups of Cyber Assets).	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA recommends clarifying that remote access clients or terminal emulators that are used to connect to a CMS are not a CMS in themselves.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Consider additional clarity on the meaning of management plane and data plane.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Please ensure the terms management plane and data plane are defined terms added to the NERC Glossary.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes

Document Name	
Comment	
While we support this concept, please see comment under question 24.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy agrees that these security controls are needed, but the requirement should be clearer on how the defined groups relate to an ESZ. If ESZ is a new term created for this type of scenario, then the requirement should refer to that term.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	

Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
By not requiring an ESZ, public power believes that this Requirement construct simplifies the requirement and provides the appropriate control objectives. The use of the word “achieve” in the draft standard sets a requirement that could be impossible to maintain as new risks emerge. Therefore, APPA proposes replacing “achieve the objective of mitigating the risks” with “address the known risks associated with,” in the standard. Additionally, public power proposes that this Requirement have the “per device capability” clause. Public power is concerned that the use of “logically separate” in this proposed requirement could redefine “logically grouped” in the BCS definition. Consequently, members would need to understand how “logically separate … into defined groups” is specifically different than “logically group.” APPA recommends that this aspect of the standard language be clarified.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	

8. Do you agree that the proposed CIP-005 Requirement R1, Part 1.7 provides a necessary security control to the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s) to reduce risks inherent to virtualization? If not, please provide a rationale to support your position.

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

Again, since it not understood what an ESZ actually is, the communication in question (if it’s not network communication) is not clear, nor are what the mechanisms to control it would be.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

A case study demonstrating the use and limitations of achieving the security objectives in a virtualized environment with existing standards should be considered before developing new standards.

Likes 0	
Dislikes 0	

Response

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light, as above, supports the concept but not the specific wording or detail. Again, Cyber Assets must be modified as "applicable" or "virtual" Cyber Assets. City Light supports APPA's simplification of this proposed requirement.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Whether Alliant Energy agrees with this requirement is dependent on clarification of the ESZ definition. Alliant Energy does agree that technical controls to enforce separation should be required.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

We recommend that the SDT consider the scoping on this requirement part. Would this be identified in the applicability table since it only applies to multi-instance? At the top of the standard/requirement? Or as shown within the requirement? We recommend the SDT provide additional clarity on the ability to have technical controls for other layers (aside from the communication layer) and with shared memory space. We would also like the SDT to consider the ramifications on the use of a cloud based SIEM vendor who is most likely using a virtualized environment. In the cloud environment, an entity would be transferring risk as well as trust

Likes 0	
Dislikes 0	

Response

John Tolo - Unisource - Tucson Electric Power Co. - 1

Answer	No
Document Name	

Comment

As above, the type of communication should be enumerated. Network and Systems engineers are aware of constructs like OSI layers and so avoiding terms like “layer 2” and “layer 3” are counterproductive in our opinion. We support the idea. We had significant internal discussion about whether you are describing a typical VMWare environment, which we consider multi-instance, or if you meant one layer removed such as Containers. The fact that we had significant internal disagreement indicates that this is unclear.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

Proposed Part 1.7 incorporated the term ESZ. See our response to the proposed ESZ definition, Question 5. Also, we do not see that the concerns regarding the proposed ESZ definition would apply any differently in proposed CIP-005 R1, Part 1.7.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC

Answer	No
Document Name	

Comment

SDG&E disagrees that the proposed control will provide necessary security controls between high and medium impact BES Cyber Systems residing in a mult-instance environment because “communications” in context of necessary inbound and outbound can mean a multitude of different types and needs of device to device or other communications. Define communications down to a much more granular level. (TCP/IP, I/O, Vsphere config, SCSI?)

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary. However, the definition ESZ should be replaced with a more general term (e.g. “Virtual Networks”).	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support the addition of Part 1.7. Reclamation recommends that revising the definition of BES Cyber System and the Impact Rating Criteria will provide sufficient security controls and reduce risks inherent to virtualization. Refer to the principles, recommended definitions, rationale, and recommended Impact Rating Criteria described in the response to Question 24.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT asserts that the intent of this requirement is unclear. The proposed ESZ appears to be focused on specific vendor technologies. Virtualization of networks verses host or integrated systems all have very different implementation based upon vendors. Adding a CMS outside of the ESP further complicates security controls.	

ERCOT requests examples of systems that can basically “firewall” non-routable protocols. Additionally, ERCOT requests clarification of an EAP equivalent for the ESZ boundary where inbound and outbound permissions can be applied. If the intention is to only refer to a routable protocol, this requirement part is redundant to the existing firewall requirement in CIP-005 Requirement R1, Part 1.3.

Likes 0	
Dislikes 0	

Response
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment
Southern Company respectfully requests additional clarity around the use of the term “communications” as it is used in the proposed requirement to achieve micro-segmentation. Does “communications” include resource usage between instances, and does it include LANs, VLANs, virtual switches, port groups, and backplane communications? Consider that for some entities, meeting strict compliance with this requirement as proposed may demand additional procurement of network virtualization solutions from vendors, such as VMWare NSX.

Likes 0	
Dislikes 0	

Response
sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment
Comments: CIP-005 R1, Part 1.7 may be a good requirement for multi-instance environments, but limiting it to virtualized systems rather than considering the proper isolation regarding communications between all virtual and physical systems may not be ideal.

Likes 0	
Dislikes 0	

Response
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment	
• The intent of this requirement is unclear. Examples of systems that can basically “firewall” non-routable protocols would be helpful. If this only refers to a routable protocol, this is redundant to the existing firewall requirement in CIP-005 Requirement R1, Part 1.3. • What is the EAP equivalent for the ESZ boundary where inbound and outbound permissions can be applied?	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Does an ESZ have to contain an ESP? Additional clarity on this aspect would be helpful.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	

Not all systems can be separated this way without introducing additional hardware such as firewalls between ESZ's. Some of the systems can be separated into ESZ's through access controls such as separating administrator roles or other methods.

TVA supports flexibility within the standard to accommodate a multi-tenant architecture and the benefits provided by adaptation of industry standard architectures such as on premises cloud computing and hyper-converged infrastructures. The ESZ concept, as presented, is overly complex, and lacks clarity to help entities how to institute separation between tenants, and shared underlying physical compute resources, whether processor (compute), storage, or transport (network). In the language provided, it is unclear as to how access control is to be executed.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST recommends simplifying this requirement to, "Implement technical controls that limit communication between separate ESZs to only that which is necessary, as determined by the Responsible Entity."

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

Refer to question #23 comments.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No

Document Name	
Comment	
This requirement implies a firewall working on routable communications. If there is a non-routable separation, the requirement is difficult to comply with. This requirement makes the demonstration of logical separation even more difficult than the logical separation in proposed CIP-005 Requirement R1, Part 1.6.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
Electronic Security Zones should already reside in separate ESPs, so the addition of this requirement should be unnecessary, unless the requirement is referring to communications such as access to the virtual console from the hypervisor and other similar communications. If it is intended to refer to those forms of communications, it needs to be clarified.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No

Document Name	
Comment	
Given that the modified Cyber Asset definition includes physical and virtual devices, this requirement will apply to physical cyber system as well, where this requirement means the current in-band network architeture is required to be redesinged. For instance, an EACMS inside ESP may require a ESZ to separate it from the BES Cyber Systems. Please clarify if SDT's intention is to apply this requirement to the virtual devices only.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
We recommend that the SDT consider the scoping on this requirement part. Would this be identified in the applicability table since it only applies to multi-instance? At the top of the standard/requirement? Or as shown within the requirement? We recommend the SDT provide additional clarity on the ability to have technical controls for other layers (aside from the communication layer) and with shared memory space. We would also like the SDT to consider the ramifications on the use of a cloud based SIEM vendor who is most likely using a virtualized environment. In the cloud environment, an entity would be transferring risk as well as trust. Baseline configuration information must be gathered and maintained for VM environment including multi-instance implementations.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
The use of an ESZ is still confusing. Rather than introduce a new concept, simply state that multiple networks (either virtual or physical) may be used in the same Shared Multi-Instance Environment (the diagram for Part 1.8 perfectly illustrates this). What then is required is that traffic between any ESP or outside of an ESP defined in the same Shared environment must implement the required security controls to enforce secured traffic between the boundaries. This then ensures that all the same controls already required for ESPs must be enforced regardless of whether it is a physical network or virtual network with physical hardware or virtualized environments.	
Likes 0	

Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
It is difficult to answer this question because it is not completely clear what the proposed R1.7 requires. Shouldn't this be "only necessary inbound and outbound communication outside the ESZ"? It seems that using "Cyber Asset(s)" could require inbound and outbound controls between two VM's in the same ESZ. The applicability for this is for BCS in a multi-instance environment. It is seems that both a single VM and an ESZ could meet the definition of "instance".	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
While we support this concept, please see comment under question 24.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
AZPS reiterates its comments regarding the revision of multi-instance to multi-tenant.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA appreciates that this is objectives-based language. Measures should be descriptions of controls used to provide the separation, not lists of inbound and outbound access ports. These are not ESPs with EAPs.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
It is difficult to answer this question because it is not completely clear what the proposed R1.7 requires. Shouldn't this be "only necessary inbound and outbound communication outside the ESZ"? It seems that using "Cyber Asset(s)" could require inbound and outbound controls between two VM's in the same ESZ. The applicability for this is for BCS in a multi-instance environment. It is seems that both a single VM and an ESZ could meet the definition of "instance".	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	

Answer	Yes
Document Name	
Comment	
We support BPA's comment.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
We agree with the direction of 1.7 but would request more details on implementation and requirements. Technical control definition could have unintended impacts and not provide any greater security controls.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

APPA suggests removing the ESZ and replacing it with “Implement technical controls that enforce only necessary inbound and outbound communication between the separated management and data planes of Cyber Asset(s) residing in a multi-instance environment.”

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	
Document Name	

Comment

The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

9. Do you agree that the proposed CIP-005 Requirement R1, Part 1.8 provides sufficient security control to reduce the risks associated with shared multi-instance environments? If not, please provide a rationale to support your position.

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

This is still not clear and does not even match the diagram given. The problem with the current definition is that it does not account for the fact that I may have multiple virtual servers on the same VLAN defined within the Hypervisor that are still in the same ESP, but not part of the BES Cyber System (e.g. a PCA that is taking advantage of the Virtual Environment). Instead, this should be used:

1. The BES Cyber System, the management plane of the shared infrastructure, and any hosted Cyber Assets not part of a BES Cyber Systems shall all be separated using an ESP defined virtually within the Virtual environment or using physical equipment linked to the virtual environment; and
2. Communications between the BES Cyber System and any hosted Cyber Assets not part of the same ESP shall all be denied by default.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

There are discrepancies between the language in the Part 1.8 and in the question. Question identifies “shared multi-instance environments “ where the requirement does not. We recommend that the SDT provide guidance on what is infrastructure (possibly using language such as BES related infrastructure) and suggest that the SDT define “Multi-instance”.

If a Jump-host (a required security control for IRA for High BESCS) which is outside of the ESP, then requirement would not be applicable. (remember that EACMs will be split—EAC and EAM). If the Jump-host was on the VM infrastructure is this a multi-instance environment?

Question—how much security do you have to implement (how many firewalls? Reside in same physical location? Trade ease of administration for security…trying to balance it; how far do you have to go to prove that it is “secured”; each environment is different.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Logical separation and “deny by default” communications are insufficient to ensure complete separation of two environments. Suggested rewording:

When an infrastructure is shared between BES Cyber Systems and other Cyber Assets not part of a BES Cyber System:

1. The BES Cyber System, the management plane of the shared infrastructure, and any hosted Cyber Assets not part of a BES Cyber Systems shall all be separated. Such separation shall achieve the objective of preventing data leakage across the separation. Such separation shall also achieve the objective of preventing code, malicious or otherwise, from migrating across the separation; and
2. Communications, if any, between the BES Cyber System and any hosted Cyber Assets not part of a BES Cyber System shall be through a defined Electronic Access Point.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Given that the modified Cyber Asset definition includes physical and virtual devices, this requirement will apply to physical cyber system as well. For the existing EACMS, PACS and PCA that are sharing the same network infrastructure, please clarify if now they need to be separated from the BES Cyber Systems. Please define what constitutes a separation and whether the separation means the authentication, inbound and outbound access control or both. Please clarify how a BES Cyber System achieves denied by default and whether it means no listening ports are allowed.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

As with the comments provided for #8 above, the term Electronic Security Zone should be explicitly used, i.e. “The BES Cyber System, the management plane of the shared infrastructure, and any hosted Cyber Assets not part of a BES Cyber System shall reside in separate ESZs”.

Additionally, this requirement does not account for Protected Cyber Assets which may need to reside within the Electronic Security Perimeter and Electronic Security Zone with the BES Cyber Assets they are associated with but do not meet the criteria for classification, or BES Cyber Assets that are treated as such because of high-water marking.

This requirement would be unecessary if the ESZ definition were amended as listed in #8 above.

Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
Although this would be acceptable for EACMS and PACS (multi-instance virtual), hardware separation should be required for BCS.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No

Document Name	
Comment	
CenterPoint Energy does not believe this requirement is necessary because part 2 of proposed CIP-005 R1.8 is redundant to the existing deny by default requirement in CIP-005 Requirement R1.3.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believe the proposed wording does not address the scenario depicted in the diagram that accompanies the narrative preceding proposed Part 1.8. Suggested rewording: “When a virtual computing infrastructure is shared between BES Cyber Systems within an ESP and other Cyber Assets outside of that ESP, the hosting virtual infrastructure shall be configured so that: (1) the infrastructure’s management plane is entirely within the ESP, (2) the infrastructure’s management plane is in a separate ESZ from both the BES Cyber Systems and other Cyber Assets that share the infrastructure, (3) communications between BES Cyber Systems and other hosted Cyber Assets that are outside of the ESP are denied by default, and (4) any and all allowed communications between BES Cyber Systems and other hosted Cyber Assets that are outside of the ESP must take place through a defined EAP."	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
TVA supports flexibility within the standard to accommodate a multi-tenant architecture and the benefits provided by adaptation of industry standard architectures, such as on premises cloud computing and hyper-converged infrastructures. The ESZ concept, as presented, is overly complex, and lacks clarity to help entities how to institute separation between tenants, and shared underlying physical compute resources, whether processor (compute), storage, or transport (network). In the language provided, it is unclear as to the target of the separation (e.g., specific groups of Cyber Assets). Policies and procedures to restrict storage of VM images and snapshots do not exist. Formal change management processes that govern image creation, security, distribution, storage, use, retirement, and destruction must be created or incorporated into the existing NERC CIP controlled change management process. Additional security monitoring and control of stored images and snapshots should be implemented. This requirement does not cover striping of BES data, where system information may cross multiple volumes and assets.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
What does the SDT mean when referencing Multi-Instance in the diagram above? Is this supposed to be referencing a cluster?	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	

Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standards Review Group has the concern with the proposed language that the drafting team is presenting at this point. From our perspective, the language is suggesting coverage of other infrastructure besides Virtualization. If that's the drafting team's intent, we recommend that the drafting team provides support details to help inform the industry on their direction for this process.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
The term "management plane" needs to be further defined in this section before being able to state agreement. The word "separated" is important and is not fully understood. Xcel Energy suggests adding the term "logically" before the term separated in #1 of Part 1.8.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	

Comment	
Comments: Frankly, it would almost be preferable that shared infrastructure not be allowed in the sense indicated, than to impose such controls on virtualized systems.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company requests additional clarification on why the management plane must reside fully within the ESP? Additionally, a description of the ESZ applicable to the example diagram would help clarify the concepts behind the proposed requirement. Southern has concerns that, if the management plane must reside fully within the ESP, the gains proposed for an Entity “to leverage the investments and protection of infrastructure shared between applicable Cyber Assets and other programmable devices” might not be realized due to the compliance burden of doing so. As stated in question 8, Part 2 of the proposed requirement needs additional clarification with regard to the use of the term “communications”. Is Part 2 of the requirement analogous to firewall rule base language, is it also applicable to shared SAN, fiber, etc. resources, and how is that expected to be implemented with regard to all forms of “communication”?	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support the addition of Part 1.8. Reclamation recommends that revising the definition of BES Cyber System and the Impact Rating Criteria will provide sufficient security controls and reduce the risks associated with shared multi-instance environments. Refer to the principles, recommended definitions, rationale, and recommended Impact Rating Criteria described in the response to Question 24.	
Likes 0	
Dislikes 0	
Response	

Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ATC proposes changing the language for CIP-005 Requirement R1, Part 1.8 #2 to say - “Communications between the BES Cyber System and any hosted Cyber Assets not part of the BES Cyber System shall be denied by default unless explicitly allowed through an EAP.” This would allow required communications for devices inside and outside of the ESP to talk to each other.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP agrees with R1, Part 1.8 as written. (Note that Transmission’s current VM environment does not have BES Cyber Systems and NON-BES Cyber Assets shared on the same Host/Hypervisor. The BES Cyber Systems are hosted on separate hypervisors (physical servers). AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
SDG&E does not agree that the proposed requirement provides sufficient security. Communications is too vague of a term, Storage is not sufficiently addressed in this control and the administrative overhead to deny by default is considerable in a shared multi-instance infrastructure.	
Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

Current Standards Already Address Risk. Proposed Part 1.8 is seeking to address the risk described and illustrated in the diagram. The risk is already addressed, or can be addressed by, using current CIP Standards.

Likes 0	
Dislikes 0	

Response

John Tolo - Unisource - Tucson Electric Power Co. - 1

Answer	No
Document Name	

Comment

We understand the intent here builds upon previous concepts, however as stated before, “separation” is too vague. Your diagram illustrates a “high watermark” approach to where you place the management system and the diagram illustrates your intent better than the words.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

There are discrepancies between the language in the Part 1.8 and in the question. The Question identifies “shared multi-instance environments“ where the requirement does not. We recommend that the SDT provide guidance on what is infrastructure (possibly using language such as BES related infrastructure) and suggest that the SDT define “Multi-instance”.

If a Jump-host (a required security control for IRA for High BESCS) which is outside of the ESP, then requirement would not be applicable. (remember that EACMs will be split—EAC and EAM). If the Jump-host was on the VM infrastructure is this a multi-instance environment?

Question—how much security do you have to implement (how many firewalls? Reside in same physical location? Trade ease of administration for security…trying to balance it; how far do you have to go to prove that it is "secured"; each environment is different.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

The separation methodology is not described in sufficient detail to determine if the security control objective is achieved.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	Yes
Document Name	

Comment

Provide clarification around the use of Virtual EAPs in the same multi-instance environment separating BCAs and non-CIP devices.

Likes 0	
Dislikes 0	

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	Yes
Document Name	

Comment

Yes, but it is unclear where the CMS should/must reside. The management plane is inside the ESP, but is the implication that the CMS is also inside the ESP or some equivalent ESZ meant for CMS?

Putting the CMS outside a protected area such as an ESP/ESZ increases the risk to the BCS and an EAP between the CMS and the management plane reduces some of the risk, but not all.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

We support BPA comment.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC

Answer	Yes
Document Name	

Comment

Request clarification of “infrastructure.” Does infrastructure refer to only the virtual environment?

Is this the “infrastructure” in the Virtualization Terms and Requirements section of the comment form which only listed virtual components? Could “infrastructure” mean the UPS systems, equipment racks, HVAC systems, floors, lighting…. The “management plane of the shared infrastructure” seems to limit and define “infrastructure” to be components of the virtual environment.

Should 1 be “logically separated” and not just “separated”?

Consider striking “by default.”

This Part is the foundation for virtualization requirements.

Likes 0	
Dislikes 0	

Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA appreciates the SDT’s effort in drafting objectives-based standards language. BPA agrees that Part 1.8 provides necessary additional security controls for shared infrastructure by separating hosted cyber assets that are not part of BES Cyber Systems as part of a comprehensive security strategy.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with CIP-005 R1.8, section 1 that there should be separation between the BES Cyber System, the management plane and any other Cyber Assets not part of the BES Cyber System. AZPS encourages the SDT to consider revising CIP-005-5 R1.1 to state that a defined ESP can exist within a multi-instance environment. In the event that the SDT retains section 2 of CIP-005 R1.8, AZPS respectfully recommends having this requirement applicable to only EACMS, CMS, and PACS, and keep CIP-005 R1.1-1.3 applicable to only high and medium impact BES Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Recommend inserting the word “logically” before separated in the Requirement.	

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	Yes
Document Name	

Comment

- Where does an ESZ apply to the diagram?
- Without this requirement, there really is no value in writing requirements for virtualization. This will help entities better utilize converged infrastructure

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

ERCOT notes that without this requirement, there really is no value in writing requirements for virtualization. This will help entities better utilize converged infrastructure. However, ERCOT seek clarification on how an ESZ applies to the diagram above.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ

Answer	Yes
Document Name	

Comment

Request clarification of “infrastructure.” Does infrastructure refer to only the virtual environment?

Is this the “infrastructure” in the Virtualization Terms and Requirements section of the comment form which only listed virtual components? Could “infrastructure” mean the UPS systems, equipment racks, HVAC systems, floors, lighting…. The “management plane of the shared infrastructure” seems to limit and define “infrastructure” to be components of the virtual environment. Should 1 be “logically separated” and not just “separated”? Consider striking “by default.” This Part is the foundation for virtualization requirements.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy agrees there should be separation between the BCS, the management plane, and any hosted Cyber Assets not part of a BCS. It should be more clear in the requirement whether separation between all 3 categories are required. Communications between BCS and non-BCS is already required go through an EAP and to be denied by default per CIP-005-5 R1.3.	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
It is not certain what is meant by “separated”. Is this meant in the networking sense? Or in an ESZ sense?	
Likes 0	
Dislikes 0	

Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
The guidance provided above in the question, states: “In order to manage Partition 2, or any Cyber Asset hosted by the multi-instance environment and outside the ESP, IP communication to the management plane from outside the ESP has to go through the EAP since the management plan of shared	

multi-instance environment has to reside inside the ESP." APPA believes that the Requirement does not address the management plane inside the ESP. Consequently, APPA believes both aspects should be included in this Requirement.

The proposed language in Question 8 would eliminate the need for the "denied by default" in R1.8.2.

The word "infrastructure" is not defined in the proposed Standard. Consequently, the "infrastructure" on page 4 appears to only include virtual components. APPA questions if this would also include the UPS systems, equipment racks, HVAC systems, floors, lighting, etc.? The "management plane of the shared infrastructure" seems to limit and define "infrastructure" to be components only of the virtual environment.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE does not have comments on this question.

Likes 0

Dislikes 0

Response

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer

Document Name

Comment

City Light, as above, supports the concept but not the specific wording or detail. Again, Cyber Assets must be modified as "applicable" or "virtual" Cyber Assets. City Light supports APPA's comments about this requirement, which also acknowledging the value of BPA's comments.

Likes 0

Dislikes 0

Response

10. The SDT asserts that the proposed CIP-005 Requirement 1, Part 3.1 provides additional security controls for remote access when performing CMS functions. These are necessary to reduce the risk associated with remote access to multi-instance environments. Do you agree with this assertion? If not, please provide a rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light generally supports the security enhancements proposed in this requirement for virtual systems, but is concerned about expanding scope for non-virtual systems (which is not the mandate of this SDT). Such changes should be handled in a more transparent manner and not included as a minor change within a major new concept.

City Light additionally supports the comments of both APPA and BPA, except as noted above.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Alliant Energy disagrees with the phrase "initiated outside of the ESZ." Access to perform CMS functions should be controlled regardless of source.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

As CIP-005 Requirement 1, Part applies to remote access, we considered that authentication takes place to the application or the management interface not to the communication. Authentication may be considered to be digital certificates for layer 2 tunnel. The requirement as written states for all sessions. Meaning each session established must perform the requirement, which may prevent an entity from using a layer 2 tunnel to perform this activity depending on particular vendor implementation.

The SDT should add Implementation Guidance that digital certificates meet the “authentication, integrity and non-repudiation controls”. The requirement does not prescribe where they have to terminate. Could be to the jump host—then connect to CMS to perform CMS functions.   If the communication is scheduled via scripts – first attempt to define either user initiated or system-to-systems communications? As it is currently written, any communication between device and CMS might have to meet the requirement. CMS should include administration….not with configuration, otherwise unintended systems are brought in (ivanti, Solar Winds)

Should include the virtual concept in that definition/term. The following is a potential definition for consideration by the SDT:

“Hypervisor or products with other similar functionality”

As CIP-005 Requirement 1, Part applies to remote access, we considered that authentication takes place to the application or the management interface not to the communication. Authentication may be considered to be digital certificates for layer 2 tunnel. The requirement as written states for all sessions. Meaning each session established must perform the requirement, which may prevent an entity from using a layer 2 tunnel to perform this activity depending on particular vendor implementation.

The SDT should add Implementation Guidance that digital certificates meet the “authentication, integrity and non-repudiation controls”. The requirement does not prescribe where they have to terminate. Could be to the jump host—then connect to CMS to perform CMS functions.   If the communication is scheduled via scripts – first attempt to define either user initiated or system-to-systems communications? As it is currently written, any communication between device and CMS might have to meet the requirement. CMS should include administration….not with configuration, otherwise unintended systems are brought in (ivanti, Solar Winds)

Should include the virtual concept in that definition/term. The following is a potential definition for consideration by the SDT:

“Hypervisor or products with other similar functionality”

A hypervisor or virtual machine monitor (VMM) is a piece of **computer software**, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor is running one or more virtual machines is defined as a host machine.

Likes 0	
Dislikes 0	

Response

John Tolo - Unisource - Tucson Electric Power Co. - 1

Answer	No
Document Name	

Comment

This would be difficult to implement in practice for many types of assets and their integrations and management systems. Non-repudiation generally requires some type of cryptographic signature and a majority of system-to-system communications inherently do not support that mechanism. Requiring it for Interactive Remote Access for a CMS makes sense, but we imagine that will be enumerated in existing standards as in-scope for CMS the way it would be in-scope for PACS, as an example.

Likes 0	
Dislikes 0	

Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
Proposed Part 1.7 incorporates the proposed terms CMS and ESZ. See our responses to the proposed CMS definition, Question 4, and the proposed ESZ, Question 5. Also, we do not see that the concerns regarding the proposed CMS and ESZ definitions would apply any differently in proposed CIP-005 R1, Part 3.1. **Alternative.** If the SDT concludes proposed Part 1.7 is required to address the identified issues, an alternative approach is to maintain the Interactive Remote Access requirements and incorporate relevant concepts contemplated by the CMS requirements.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
See earlier requirement of clarification of where the CMS resides in this control as well as stronger definition of non-repudiation of system-to-system communication.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary. However, further clarification is needed for the terms “Authentication, Integrity, and Non-Repudiation” in the compliance guidance.	

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ

Answer	No
Document Name	

Comment

Is this redundant with CIP-005, Requirement 1, Part 1.3?

Request specifics on “authentication, integrity and non-repudiation controls.”

Please clarify if non-repudiation controls is a technical control. If YES, are we moving too far away from outcome based controls?

This requirement may need to include the “per device capability” phrase.

Likes 0

Dislikes 0

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support the addition of Part 3.1. Reclamation recommends that revising the definition of BES Cyber System and the Impact Rating Criteria will provide sufficient security controls to reduce the risk associated with remote access to multi-instance environments. Refer to the principles, recommended definitions, rationale, and recommended Impact Rating Criteria described in the response to Question 24.

Likes 0

Dislikes 0

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT asserts that this requirement is redundant to the existing firewall requirement in CIP-005 Requirement R1, Part 1.3. As written, ERCOT offers the following comments. (1) The requirement lacks complete and appropriate details necessary for evaluation and implementation. (2) The requirement may create conflict with existing CIP Version 5/6 implementations. (3) While the security controls may be appropriate, the technologies may not support all or some of the requirement. Clarification for network verses host technologies is required. (4) The requirement does not specify it is for multi-instance. (5) The SDT should be specific about the meaning of “authentication, integrity and non-repudiation controls”. Are these existing controls in the CIP standards for non-virtual systems? (6) With non-repudiation, the SDT appears to be adding an additional requirement for key management that is not clearly stated. (7) As noted in question 8, ERCOT requests examples of systems that can basically “firewall” non-routable protocols. ERCOT recommends the creation of ERO-endorsed guidance before standards to aid in evaluating options. The guidance can document the implementation under various vendor and technology types.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Comments: Singling out virtualized environments for special controls seems unnecessary. Surely remote access rights and rules could be based on the nature and quantity of what cyber assets could be affected regardless of their physical or virtual nature.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	

- This is redundant to the existing firewall requirement in CIP-005 Requirement R1, Part 1.3.
- Examples of systems that can basically “firewall” non-routable protocols would be helpful.
- The requirement does not specify it is for multi-instance.
- Be specific about what is meant by “authentication, integrity and non-repudiation controls”. Are these existing controls in the CIP standards?
- With non-repudiation, are you requiring key management, etc. in a backdoor manner?

Likes 0

Dislikes 0

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE

Answer No

Document Name

Comment

Not sure how "non-repudiation controls" applies in this part 3.1. Xcel Energy suggests that the term "integrity" be further defined. For example, does it mean traffic must be encrypted or does it have other mechanisms to validate and authenticate the communication? Additional technical guidance will be needed to understand the differences between this and Interactive Remote Access.

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer No

Document Name

Comment

The SPP Standards Review Group has a concern on how the terms “ESP” and “ESZ” are used in this section of the documentation while discussing the risks associated with communication. At this point, we feel that there is no consistency in reference to the use of the terms. For example, the supporting details for the section mentions “ESP” while language in Part 3.1 mentions “ESZ”.

Question:

What are the drafting team’s expectation in reference to meeting the compliance need of the terms “integrity” and “non-repudiation” controls?

Will the drafting team have the expectation of all system to system communication outside of the ESZ to communicate with system inside of the ESZ to be encrypted?

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
Consider defining “integrity” and “non-repudiation controls” in the context of this Requirement.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	No
Document Name	
Comment	
Is this redundant with CIP-005, Requirement 1, Part 1.3? Request specifics on “authentication, integrity and non-repudiation controls.” Please clarify if non-repudiation controls is a technical control. If YES, are we moving too far away from outcome based controls? This requirement may need to include the “per device capability” phrase.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	

TVA requests additional context for understanding the proposed requirement. If an entity has multiple ESZs and/or ESPs, it is unclear how an entity would satisfy the proposed language. Network traffic traversing does not identify itself on a technical level as being interactive or machine-to-machine. Unless an entity has implemented software defined networking, which can associate traffic flows to and process identity end-to-end, it is difficult to envision a technical solution that satisfies the draft language.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

While N&ST agrees there should be strong technical and procedural protections around hypervisors, N&ST does not believe this goal is well-served by the proposed requirement and is not convinced there are “gaps” in the current requirements for Interactive Remote Access. In addition, N&ST notes:

(1) The narrative section preceding the proposed requirement discusses CMS access from outside an ESP, whereas the proposed requirement language says, “ESZ.”

(2) Authentication is already required for access by human operators.

(3) System-to-system communications from outside an ESP are already subject to controls implemented by EAPs.

(4) It is unclear what type of “integrity” control(s) the SDT envisions in this context.

(5) It is unclear what goal(s) would be served by “non-repudiation,” nor is it clear how it might be achieved in this context. Perhaps all CMS transactions should be logged, with an accompanying requirement that the entity be capable of determining what individual or system initiated any given recorded transaction.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

Refer to question #23 comments.

Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy does not agree with the proposed requirement because of the difficulty in implementation and demonstration of compliance. It is not clear how an entity can distinguish between sessions used for CMS functions and those that are not. Further, it may be challenging to distinguish between user initiated and system-to-system sessions, when such communications are allowed between the hosts, ports, and applications involved. Further, it does not account for system capability. The requirement can be even more challenging to comply with if the logical separation in the ESZ is not through a firewall.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	

There has not been enough definition around ESZ’s and if they exist inside or outside of a ESP. The required controls are vague and poorly defined. We do not recognize a gap in the intermediate system. The CMS should always reside inside the ESP on separated hardware. This alleviates the remote access to perform CMS function gap.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

The language of the proposed requirement is unclear as to what communications this applies to. Does it apply to the client connection to the CMS, or to the CMS connection to the BES Cyber Asset? The language of this requirement is also not consistent with the rationale given, as the rationale describes issues with communications from outside the ESP, but the requirement addresses the ESZ.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

The gap identifed by the STD is not defined and needs further clarification. As we proposed EACMS modification that includes CMS in question 4, this requirement is not necessary since the current EACMS requirements can meet this.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

As CIP-005 Requirement 1, Part 3. Applies to remote access, we considered that Authentication takes place to the application or the management interface not to the communication. Authentication may be considered to be digital certificates for layer 2 tunnel. The requirement as written states for all sessions. Meaning each session established must perform the requirement, which may prevent an entity from using a layer 2 tunnel to perform this activity depending on particular vendor implementaions.

The SDT should add Implementation Guidance that digital certificates meet the “authentication, integrity and non-repudiation controls”. The requirement does not prescribe where they have to terminate. Could be to the jump host—then connect to CMS to perform CMS functions. If the communication is scheduled via scripts – first attempt to define either user initiated or system-to-systems communications? As it is currently written, any communication between device and CMS might have to meet the requirement. CMS should include administration….not with configuration, otherwise unintended systems are brought in (ivanti, Solar Winds)

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

It is acceptable if ESZ was replaced with ESP.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
We do agree that Part 3.1 provides additional security controls for remote access; however, the Applicable Systems should be updated to say "high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s)".	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that controls are necessary, but do not feel that the proposed language clearly explains what controls should be implemented, and where said controls should be implemented as well. As written, it isn't clear what the SDT intends to be implemented.	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA appreciates efforts to align NERC CIP standards with recognized cyber security principles and objectives.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Stronger language is needed to bring authentication up to at least the level required for Interactive Remote Access.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
Yes but this may not be enough – e.g., the system-to-system communications between an out of ESZ CMS and the management plane may in fact meet all of the items in part 3.1, but if the CMS is already compromised (which is more likely if it is not in the ESZ) then these controls do nothing to prevent the attacker controlling the CMS from causing damage.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	

Public power believes that this Requirement conflicts with the implied requirement identified in comments to question 8 that the management plane of the BCS must be inside the ESZ. APPA recommends replacing the proposed language with: “Require authentication, integrity and non-repudiation controls for all CMS functions, per device capability.”

If the suggested modification is not used, in the alternative APPA proposes that this Requirement have the “per device capability” clause.

Encryption of network traffic form CMS to device could make compliance with this Requirement impossible to achieve.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	
Document Name	

Comment

The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

11. Should the gap between Interactive Remote Access and system-to-system communication that was exposed by the examination of the risks inherent to virtualization be addressed for systems other than high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS? If not, please provide a rationale to support your position.	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
This question is unclear – please provide clarification. Is this about Lows? Is it about non-multi-instance Highs and Mediums? Both? Etc.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We proposed EACMS modification including the cyber system that can alter the configuration of BCS regardless of whether it has IRA or system-to-system access to the BCS that resides inside or outside ESZ.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
System-to-system communications should be addressed the same as CIP-005-5 R2.	
Likes 0	
Dislikes 0	

Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
SDT’s example of CMS in a virtualized high/medium impact environment should not be permitted.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes the requirement should be limited to the highest risk BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

TVA requests that any controls associated with the use of a CMS apply to individuals' access to the CMS itself, rather than the network traffic that may originate from a CMS to an applicable BES Cyber Asset. Network traffic traversing does not identify itself on a technical level as being interactive or machine-to-machine. Unless an entity has implemented software defined networking which can associate traffic flows to and process identity end-to-end, it is difficult to envision a technical solution that satisfies the draft language. As a case study, consider a CMS tool used to manage network devices (e.g., routers, firewalls, switches) via SSH. The tool may have a daily backup configured whereby it initiates an SSH session to a target device for the purposes of collecting a complete device backup. The SSH traffic, from a firewall and access control perspective, cannot be identified as “machine to machine”, even though no human is interactively driving the SSH session. However, the same CMS tool may facilitate real time, Interactive Remote Access to a target device where each command was issued by a human facilitated by an SSH connection. From a network perspective, the SSH session’s origin as human or machine-to-machine is indistinguishable.

TVA suggests a more effective manner to address these concerns would be to utilize controls similar to those used for gaining access to an Intermediate System for remotely gaining access to a CMS.

Finally, TVA suggests the concerns about “the gap between Interactive Remote Access and system-to-system communication” are not proprietary to virtualized environments. The use of CMS tools can be manifest with or without virtualized technologies.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS agrees that the gap should be addressed for the applicable systems that are high and medium impact BES systems, but does not agree that the gap should be addressed for low impact BES cyber systems.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment	
The gap between Interactive Remote Access, and system-to-system communication does not need to be addressed for systems other than high and medium impact BES Cyber Systems. Outside of the multi-instance environment, the risk associated with system to system for individual discrete assets is limited to within the company’s environment. Anything outside of the company’s environment should be covered under CIP-012.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
There is not an inherent risk for system-to-system communication. If the gap is addressed, please ensure that the compliance Requirements do not apply to Low Impact BES Cyber Systems nor to systems that are out-of-scope.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	
IRA only applies to Cyber Assets within an ESP. Requiring this for EACMS will lead to the “hall of mirrors” issues. This is another reason that CMS devices should be classified as a BCA if they support a BCA.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	

Comment	
Comments: It would seem wise to resolve issues with high and medium impact BES Cyber Systems before addressing low if there is inherent risk to virtualization greatly exceeding that posed by any systems using shared resources whether physical or virtual. The idea occurs that the inherent potential reduction in risk provided by virtualization be properly weighed as well as so much redundancy can be built into these systems.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT notes that Interactive Remote Access only applies to Cyber Assets within an ESP. Requiring this for EACMS will lead to the “hall of mirrors” issues. This is another reason that CMS devices should be classified as a BCA if they support a BCA.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends the requirements addressing the risks inherent to virtualization apply only to high and medium impact BES Cyber Systems residing in Multi-Virtual Instance environments and their associated Virtual Centralized Management Systems (VCMS). Refer to the recommended terms and definitions in the responses to Questions 4 and 6.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No

Document Name	

Comment

AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

The question incorporates the proposed CMS term. See our response to the proposed CMS definition, Question 4.

Also, Standards are to address risk but cannot address every iteration of risk. To develop requirements to address every security risk is not sustainable and an unreasonable expectation. Security threats emerge more quickly than can be addressed by a process of law.

Likes 0	
Dislikes 0	

Response

John Tolo - Unisource - Tucson Electric Power Co. - 1

Answer	No
Document Name	

Comment

See comments for #10.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	No

Document Name	
Comment	
Risk based assessment.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
It needs to be addressed for any virtualized PCA, PACS or EACMS as they pose similar risks. It should also be addressed for any similar communications in non-virtualized systems – e.g., a lights out management system for servers or a network management system. These pose similar risks to the BCS they support. This may not be enough to protect the BCS appropriately.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	

Comment	
All Cyber Assets in a multi-instance environment and their associated CMS should rise to the highest watermark level in order minimize/mitigate potential risks of cross system compromise.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	Yes
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Although N&ST is not necessarily convinced at this time that additional controls are needed for system-to-system communications between BES Cyber Systems and Cyber Assets outside of ESPs, we believe it nonetheless makes sense to examine the question while it is being considered for BES Cyber Systems running in virtual environments.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
We support the concept of reducing the risk associated with remote access (both system-to-system and Interactive); however, we believe those requirements should be appropriate to the risk level of the Cyber Assets (we believe you are looking to address EACM, PACS and Low Impact BES Cyber Systems).	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes

Document Name	
Comment	
There is an opportunity to extend these controls out to the CMS of virtualized PACS and EACMS.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
City Light agrees additional known risks should be addressed, but disagrees that the virtualization changes are correct forum to make such changes (because of the complexity of the changes for virtualization and the great likelihood that the other changes will be lost in the chaff).	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
The NERC standards should be written to address the known risks and not limited to risks associated with managing multi-instance environments.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time	
Likes 0	
Dislikes 0	
Response	

12. The SDT asserts that the new proposed CIP-004 Requirement R4, Part 4.5, provides additional security control to the electronic and unescorted physical access to multi-instance environment processes which reduces the “too much privilege” risk inherent to virtualization which has been identified. Do you agree with this assertion? If not, please provide a rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light agrees with the general principles esoused in this new requirement but finds it, as worded, to be too vague and too subject to auditor intepretation.

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

We recommend the addition of “Per system capability” similar to “per device capability”.

Does the SDT consider that AD provides enough of these controls? Can it do “need-to-know, least privilege, and separation of duties”?

Could this requirement part be include with the current CIP-004 R4 Part 4.3 review? Will the applicability extend to BCS and associated EACMs? Associated PACS?

We recommend that this become Requirement 4 Part 4.2 as the Authorization takes place in 4.1; implementation should become 4.2; then the quarterly review is 4.3, etc. We recommend that the SDT shift the CIP-004 R4 Parts to have the steps occur in order of operation. We recommend that the SDT provide guidance to small entities that they may identify each role but may need to (resource constrained) add the same person to each role

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

Current Standards Already Address Risk. Proposed Part 4.5 is not significantly different from existing CIP-004 Part 4.1 which already requires a process to authorize based on need.

Compliance Uncertainty. The terms “need-to-know,” “least privilege,” and “separation of duties,” are currently used in the Standards and, also, open to a broad level of interpretation; as such, they create compliance uncertainty. It is expected that will not change.

We do not believe additional prescriptive language or defining the terms is sufficient to mitigate the uncertainty.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC

Answer	No
Document Name	

Comment

SDG&E seeks to understand where ERC fits into this proposed requirement.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

AEP believes the existing requirements can be determined to be applicable in a virtual environment by a reasonable person. New requirements are not necessary.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	No
Document Name	
Comment	
This Requirement seems to expand the scope of Requirements 4.1 – 4.4. The question asks about “multi-instance.” We recommend the applicability section should be similar to CIP-005 R1.8 It is unclear why virtual systems need additional physical access to the virtual systems. Request clarification of “separation of duties.” The entity, as part of their “based on need” approval process for 4.1 could include need-to-know, least privilege, and separation of duties “. This added requirement seems like additional administrative tasks and extends to all BES Cyber systems and not just virtual systems.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
The proposed addition of CIP-004 Requirement R4, Part 4.5 is too broad, and applies to everything including virtualization. If the SDT is trying to reduce the “too much privilege” risk inherent to virtualization, the requirement should be specific about virtualization privileges. As proposed, entities would have to apply these security controls to all BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support the addition of Part 4.5. Reclamation recommends that revising the definition of BES Cyber System and the Impact Rating Criteria will provide sufficient security controls and reduce the “too much privilege” risk inherent to virtualization. Refer to the principles, recommended definitions, rationale, and recommended Impact Rating Criteria described in the response to Question 24.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT asserts that the concept noted in this requirement should not be added at all. It is redundant and unneccessary. The proposal is too specific and will create adverse impact to many existing implementations without improving the security desired. Entities with high and medium impact BES Cyber Systems already have to provide justification for access at least every 15 months. Entities are required to provide evidence supporting that access is (1) necessary, and (2) for performing assigned work functions. These two criteria should be seen as the obligation to address the principles of need-to-know, least privilege, and separation of duties. Any further clarification should be made in implementation guidance.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern disagrees with the need for this additional requirement under CIP-004-6 R4. First, existing CIP requirements under CIP-004-6 R4 already require the authorization of access based on need, and it is not necessary to repeat that tenant of cyber security in another requirement. When implementing ‘principles’ of least privilege and separation of duties, that can be exhibited in various ways to meet the needs of an Entity’s operations while maintaining adequate security. The currently proposed requirement leaves too broad a level of ambiguity to auditor interpretation regardless of an Entity’s efforts to comply. Additionally, as stated, “The SDT has identified “too much privilege” as an inherent risk in virtualization”, however the proposed requirement in not scoped to virtual environments and would be applicable across the board. All of CIP-004-6 R4 is currently scoped to High

Impact BES Cyber Systems and Medium Impact BES Cyber Systems with ERC – and Southern requests explanation on why the ERC scoping for Mediums would be excluded in this context.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Comments: Singling virtualized environments out for special RBAC consider seems counter-productive. Certainly appropriate access should be justified and reviewed wherever it is granted.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

The Applicable Systems of this requirement should be updated to say “high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s)”. Additionally, BES Cyber System Information should be changed to “designated storage locations for BES Cyber System Information” to align with CIP-004 Part 4.1, Part 4.4 and Part 5.3. Furthermore, the currently approved requirement CIP-004 Part 4.1 incorporates the concept of “need”. We feel that adding this new requirement is a duplication of the already existing requirement of need and provides a chance of double jeopardy for the entities and should be removed.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

The concept noted in this requirement should not be added at all. It is redundant and unneccessary. Entities with high and medium impact BES Cyber Systems already have to provide justification for access at least every 15 months. Entities are required to provide evidence supporting that access is (1) necessary, and (2) for performing assigned work functions. These two criteria should be seen as the obligation to address the principles of need-to-know, least privilege, and separation of duties. Any further clarification should be made in implementation guidance.

Likes 0

Dislikes 0

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE

Answer	No
Document Name	

Comment

As written, Part 4.5 goes beyond the scope of addressing virtualized environments.

Likes 0

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standards Review Group has a concern that the proposed language presents redundancy issues. Additionally, we feel that the topic is already covered in the CIP-004 Standard section 4.1 and should not be added to the Virtualization process.

Question:

With this proposed language, who will be impacted by the applicability?

Likes 0

Dislikes 0

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
While Duke Energy agrees in principle, we cannot agree with the language proposed for Part 4.5. Currently, it isn't clear what duties would need to be separated under Part 4.5. We suggest adding language or providing additional rationale that would address specifically what is to be separated.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
While AZPS agrees with the intent to protect BES Cyber Assets and BCSI, it suggests that the proposed R4.5 is not as clear and unambiguous as it could be and, therefore, could result in confusion regarding applicability. To ensure that the scope of the requirement is clear, AZPS recommends that the language of R4.5 specifically reference virtual, multi-tenant environments. Additionally, while AZPS understands and acknowledges the value of the concepts of need-to-know, least privilege and separation of duties from a security perspective, AZPS cautions the drafting team regarding the cost/benefit ratio of including separation of duties in R4.5. In particular, AZPS is concerned that the inclusion of separation of duties would represent a significant cost impact to the Responsible Entity for very little attendant benefit to reliability.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Some organizations may lack staff to separate duties to multiple people. Additionally, the requirement does not establish a measureable span of control. The current CIP-004 requirements sufficiently address the need to implement an effective access control policy to limit privileges using these principles.	
Likes 0	

Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes that “need-to-know” and “least privilege” are already addressed by CIP-004 R4. N&ST also believes that while separation of duties is an important security practice, it may be impractical or prohibitively costly for small entities with small IT or OT staffs.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Refer to question #23 comments.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes the proposed requirement is more of a best practice and should not be a requirement. Existing CIP-004 requirements already require authorization of access based on need. Similar to the language in proposed CIP-005 Requirement 1, Part 1.6, this requirement asserts an objective to the requirement, where evidence of objectives (or principles) is difficult to provide compared with evidence of activities. The proposed CIP-004 Requirement 4, Part 4.5 will be challenging to implement for smaller entities with limited staff, where the level of separation “in principle” cannot be achieved to satisfy the requirement.	

Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
Part 4.5 does not address virtualization or segmentation of duties for virtualization management. However, in a shared environment, processes would need to be created or authorizations changed and documentation would need to spell out duties and access. There should be more guidance and direction on what is appropriate separation of duties.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
Groups that manage CIP systems are often small and cannot easily address separation of duties or least privilege without undermining reliability. This would be a documentation exercise that would provide no additional security.	

Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Please clarify if this proposed Part 4.5 is going to replace the current Part 4.1 since they are overlapped.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
We agree with this as written explicitly because it allows us to make a determination of what “need-to-know” and “least privilege” means to us. If there will be additional guidance or directives then that guidance or directive might change our viewpoint. We support the concept as a basic security tenant.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	

Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
We recommend the applicability section should be similar to CIP-005 R1.8 This Requirement seems to expand the scope of Requirements 4.1 – 4.4. Request clarification of “separation of duties.”	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
The terms “need-to-know,” “least privilege,” and “separation of duties” need to be defined in the Glossary or carefully explained in Implementation Guidance.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	

Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
We agree with this statement and it is good that it is not restricted to virtualized environments. This problem exists in many traditional environment as well, and it is addressed appropriately by the new requirement.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	

The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

13. Do you agree with the SDT's assertion that the definition of EACMS is too broad and does not differentiate the capabilities and risk(s) of the systems that fall within that definition scope? If not, please provide rationale to support your position.

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

Existing definition is adequate.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

We potentially agree given that it might require protection for some systems that do not require the higher level of protection. Electronic Access Control (real time) has more risk than Electronic Access Monitoring (after the fact)

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Actually the current EACMS definition implies that a Cyber Asset that has directly electronic access to the BCS is supposed to be identified as EACMS since it controls access to the BCS. We have proposed a modified EACMS definition in question 4 to include SDT proposed CMS.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

All EACMS's and CMS's, and ESZ's, etc. should be afforded equal protections to the highest watermark level within the associated environment. The compromise of one or more BCS's/BCS's (and/or associated systems) i.e. compromise of information, or ESP, or CMS can have an adverse effect on the BES regardless of the number or type of asset compromised.   The risks may seem different however; the BES would be impacted in some way.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy believes the existing EACMS definition should be clarified for EACMS used for access monitoring. CenterPoint Energy proposes the following clarification:

"Cyber Assets that perform electronic access control **or are used for** electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems."

Some misinterpretation of EACMS is based on capability, rather than use, of tools where no access monitoring is intended. A system that is actually used and intended to capture all access activity should also be protected as other systems in scope for EACMS due to the risk posed by compromise of those systems. A tool used for monitoring configuration with no system management capability, antivirus, or security functions other than access control with some limited capability to pick up information related to access control should not be considered access control systems.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

We do not believe that the EACMS definition is too broad.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes that both the current definition of EACMS and the requirements applicable to such devices are adequate and appropriate within the context of requirements applicable to high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standard Review Group feels that the current definition gives the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	

The EACMS definition is broad. However, the use of a single category allows entities to define a single set of controls for all systems in the category. This simplifies security and compliance obligations.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
All EACMS's and CMS's, and ESZ's, etc. should be afforded equal protections to the highest watermark level within the associated environment. The compromise of one or more BCS's/BCS's (and/or associated systems) i.e. compromise of information, or ESP, or CMS can have an adverse effect on the BES regardless of the number or type of asset compromised. The risks may seem different however; the BES would be impacted in some way.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT agrees that the EACMS definition is broad. However, the use of a single category allows entities to define a single set of controls for all systems in the category. This simplifies security and compliance obligations.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation supports the current definition of EACMS; applicable requirements that address risk(s) are determined by the Impact Rating Criteria.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes that fewer higher level definitions provide needed flexibility to responsible entities, employing a security mindset, in establishing required security for their BES Cyber Systems. We also agree that devices currently classified as EACMS, but with no ability to control access should be classifiable as BCSI repositories. We also agree with the introduction of the CMS definition. However, the other definitions are not necessary at this time.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The current EACMS elements are sufficient in providing implementation structure and flexibility to ensure security and address the differences found in entities' system designs without highly prescriptive Requirements. **Alternative.** Should the SDT seek to restrict the EACMS definition, we encourage any revisions maintain flexibility in consideration of different system designs to allow entities to address those differences in implementation and compliance activities.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No

Document Name	

Comment

This adds significant complexity to the discussion. We prefer to assign a higher and more consistent security strategy based on a single categorization rather than juggle requirements which are likely to be highly similar or even implemented to the higher level out of a desire to be more secure.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

Cowlitz supports BPA comment.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

TVA supports the SDT's efforts to differentiate the categorizations of EACMS components based on the ability of such systems to affect access control and/or real time BES Cyber System functionality.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
We agree that the NERC standards need to allow for the level and type of monitoring described here. It seems that EACMS would need to be replaced by the combination of EAG, EACS and the BCSI changes and not left in place.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
EACMS includes too many different functions to have prescriptive requirements applied broadly. Additionally, the requirements currently discourage entities from using vendor-based security monitoring services that could provide significant security benefit. At a minimum, monitoring systems (logging and event monitoring) that have no technical capacity or permission to configure BCSs should have risk assessed differently. There may also be value in separating security objectives between access control (authorization and permissions) and gateway functions (filter/forward traffic).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	

Comment	
We agree that the NERC standards need to allow for the level and type of monitoring described here. It seems that EACMS would need to be replaced by the combination of EAG, EACS and the BCSI changes and not left in place.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
We potentially agree given that it might require protection for some systems that do not require the higher level of protection. Electronic Access Control (real time) has more risk than Electronic Access Monitoring (after the fact) TEC recommends that the SDT consider guidance to explain what does pose a security threat. We suggest consideration that "Information to plan or execute an attack….." is appropriate, but that pose a security threat is too general." Starting point for definition: Information that is not on an asset that is afforded NERC protections. Where is the question on BCSI definition? We believe that the SDT should be asking for industry input on the proposed changes to BCSI as well as the proposed terms.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
City Light supports BPA's comments. City Light however remains concerned about the breadth and scope of the changes, and urges careful consideration by the SDT, by registered entities, and by NERC and the Regions that the impact of the proposed changes is well understood and mapped prior to adoption.	
Likes 0	
Dislikes 0	
Response	

Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	
Document Name	

Comment

The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE does not agree that the definition is too broad and suggests the current definition affords the necessary flexibility for registered entities to implement its cyber security program.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	
Document Name	

Comment

No comment at this time.

Likes 0	

Dislikes 0	
Response	

14. Do you agree that the language of the proposed definitions of EACS provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

The proposed definition provides more clarity but has its own set of issues: Hall of mirrors—"this includes Intermediate Systems" should be removed. The definition needs to be clear enough to indicate that an intermediate system needs to be covered.

That being said, the current definition of an Intermediate System states that it can't be inside the ESP. The new EACS does not apply 5.1 correctly. We suggest adding a "one pass rule" so that entities don't have to go through the requirements multiple times.

In addition, we believe that requirements should not put additional controls on top of a security control. If there is a need to do that, the additional controls need to be based on risk.

We also encourage the SDT to consider using an approach similar to that used for CIP-014 (NIST allows that as well…develop security controls): Requirement 1: Here are the minimum requirements. Requirement 2: address security risks that are not addressed that are not covered above.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

We can see some value from the proposed EACS definition but struggle in identifying how it supports security and reliability issues that are already addressed in the current Standards. The concern is adding EACS as another NERC Glossary Term will create unnecessary compliance and implementation complexity. When taken in total with all the proposed new and revised Glossary Terms and Requirements presented in this commenting form, the cumulative and gross effect is increased complexity with, likely, marginal improvement in security or reliability.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No

Document Name	

Comment

While the definition of EACS further refines an approved, AEP requests the SDT refer to our response to Question #13.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support a new definition of EACS. Reclamation recommends the SDT use existing industry-recognized terms to address the components of EACMS that control and authenticate electronic access, such as firewall, proxy server, router, etc.

If the SDT decides to use the proposed definition of EACS, Reclamation recommends the proposed EACS definition be changed

from: Cyber Assets that perform electronic access control of the BES Cyber Systems. This includes Intermediate Systems.

to: Cyber Assets that control electronic access to BES Cyber Systems.

Reclamation also recommends the SDT change the definition of BES Cyber System as described in the recommended definitions section of the response to Question 24.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT considers the EACS definition to be a good concept. However, the concept should be incorporated into a single comprehensive definition along with CMS and EAG.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

While we agree with the concept of separating out monitoring and control we do see some possible confusion with the EACS and EAG definitions. We believe that there may be instances where a system or asset performs both functions. How would you classify and protect this device? Additionally, it appears from the chart above, “Proposed Requirements Related to EACMS Changes”, that all updated requirements for EACS and EAGs are applicable to the same requirements. For simplicity purposes, we suggest that EACS and EAG be combined into one definition: “Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

This is a good concept and should be incorporated into a single comprehensive definition along with CMS and EAG

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standard Review Group feels that the current definition gives the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

The proposed definition of EACS appears vague, and would benefit from additional language in the text of the definition. We recommend inserting some of the language used in the paragraph below the proposed definition, to be inserted in the text.

See example below:

- *Electronic Access Control System (EACS):*

Cyber Assets that perform electronic access control, and authentication and authorization of traffic or users of the BES Cyber Systems. This includes Intermediate Systems.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

While AZPS agrees with the proposal to differentiate control and monitoring, AZPS is concerned that monitoring includes more than data collection and storage. For example, alerting occurs utilizing inputs from monitoring and may occur concurrently in the same system. Accordingly, the alerting and monitoring systems may not be completely independent. For this reason, AZPS recommends that the SDT give some additional consideration to the proposal to ensure that all aspects of monitoring and dependent processes are fully evaluated and addressed.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No

Document Name	
Comment	
TVA agrees that the language provides more clarity, but the term “pose a security threat” needs additional explanation. Does this term mean any security threat, or does the requirement allow the registered entity to determine a risk tolerance for the data? With all of the information that is excluded, what data remains to be considered BES Cyber System Information? The only remaining data for consideration would be user names, passwords, and security vulnerability information.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes the proposed definition of “EACS” is an unnecessary derivative of “EACMS” that provides no benefit. Furthermore, the proposed definition fails to address access control of Electronic Security Perimeters.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
We do not believe a change is necessary.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No

Document Name	
Comment	
CenterPoint Energy does not agree with the proposed definitions EACS or EAG. The existing definition of EACMS is sufficient with the added language suggested in #13. The intent, to distinguish authentication activity with packet inspection and filtering activity, is not stated in the proposed definitions. The separation into EACS and EAG might be better achieved by defining “access control” as either user/credential authentication or filtering performed at an EAP.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree to break the EACMS into three terms. This change would cause more changes and more additional work for reclassification with little compliance work reduction.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No

Document Name	
Comment	
The proposed definition provides more clarity but has its own set of issues: Hall of mirrors—“this includes Intermediate Systems” should be removed. The definition needs to be clear enough to indicate that an intermediate system needs to be covered. That being said, the current definition of an Intermediate System states that it can’t be inside the ESP. The new EACS does not apply 5.1 correctly. We suggest adding a “one pass rule” so that entities don’t have to go through the requirements in multiple pases as they are currently doing. In addition, we believe that requirements should not put additional controls on top of a security control. If there is a need to do that, the additional controls need to be based on risk. We also encourage the SDT to consider using an approach similar to that used for CIP-014 (NIST allows that as well…develop security controls): Requirement 1: Here are the minimum requirements. Requirement 2: address security risks that are not addressed that are not covered above.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
Keep current EACMS definition.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
City Light supports BPA's position and comments.	
Likes 0	
Dislikes 0	

Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
The definitions themselves seem reasonable and understandable.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
Yes, as long as the concept of monitoring is also changed to solely be the classification of the monitoring data as BCSI, when applicable. We do not think the all monitoring data would meet the BCSI definition. Ie. video recording of a single door.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
While ATC agrees with the proposed definition of EACS, there is some concern that if there is a requirement to put an EACS inside the ESP, it could result in complex configurations making security more difficult.	
Likes 0	
Dislikes 0	
Response	

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Yes, the proposed language provides more clarity, but public power would note that the change includes intermediate systems.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA also recommends clarifying that AAA clients that subscribe to EACS/AAA services (e.g., via a protocol such as LDAP, RADIUS or TACACS+) but do not maintain any account information are not EACS themselves.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	

Answer	Yes
Document Name	
Comment	
Yes, as long as the concept of monitoring is also changed to solely be the classification of the monitoring data as BCSI, when applicable. We do not think the all monitoring data would meet the BCSI definition.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Should be added as part of the EACMS definition.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment
Texas RE does not have comments on this question.

Likes 0	
Dislikes 0	

Response
Richard Vine - California ISO - 2

Answer	
Document Name	

Comment
The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

15. Do you agree that the language of the proposed definitions of EAG provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

Keep current EACMS definition.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

Comments: We think that the SDT is attempting to differentiate hardware from virtual environment. The EAG hosts the EAP makes it seem that it is virtual. Some entities share a concern that the EACS and EAG are the same; is the EACS addressing lateral movement? Part 1.5 is applicable to EAPs for high & medium at control centers. With the new definition, will that no longer be applicable for EAPS?

Is the BES Cyber Asset an EACS? Is it physical or virtual? Is the implication there that it is both? (for example: Domain controllers/TACACS) This creates an implementation challenge for entities given the dual nature of some devices.

An Electronic Access Gateway hosts the EAP and performs the active function of filtering or forwarding traffic at the demarcation point (boundary protection). Primarily, these are firewalls and routers that perform gateway functions at the layer 3 ESP boundary demarcation point. Separation of duties issues here?

The EAG hosts the EAP…makes it sound as if it is virtual. Internal discussions raised the question of whether the Electronic Access Gateway term is required.

Cisco FW is more virtual; Checkpoint the language makes sense; Checkpoint offers IPS to run in parallel; or in line IPS appliance

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with this. See the same comments as in question 14.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
This appears to be an unnecessary segmentation of an EAP, unless there is clarification provided that this is referring to a virtual firewall and the EAG is the physical host and the EAP is the virtual firewall running on the host.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No

Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy does not agree with the proposed definitions EACS or EAG. The existing definition of EACMS is sufficient with CenterPoint Energy's added language in the response to Question No. 13. The proposed EAG definition creates a risk that requirements restricted in scope with the granular description of an EAP as a specific interface will be reinterpreted to apply an entire gateway or group of gateways. The EAG concept also encourages entities to employ dedicated CIP gateways to avoid confusion, which runs counter to the move to multi-instance environments.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
We do not believe a change is necessary.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No

Document Name	
Comment	
N&ST believes the current definition of EACMS adequately applies to devices that have one or more interfaces that act as Electronic Access Points.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
TVA suggests the overlap between the term Electronic Access Point and EAG is unclear. Please consider consolidating the terms.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes the EAG definition is too similar to the EACS definition to be useful. The EAG definition should explicitly reference the filter/forward function rather than state “perform electronic access control.” Proposed: EAG - Cyber Assets that perform filtering or forwarding of traffic at the Electronic Security Perimeter(s) OR between ESZs. The EAG also hosts the EAP(s) if any.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	

Answer	No
Document Name	

Comment

The use of the term “hosts” in the proposed language is vague. We suggest the following alternative language:

- *Electronic Access Gateway:*

Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s). The Electronic Access Gateway exists on the EAP(s).

We believe the phrase “exists on” rather than using the word “hosts” is more appropriate in this context.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The SPP Standard Review Group feels that the current definition gives the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

There is no need to have a separate definition for EACS and EAG if they are both providing access control functions. The differentiation of controls is not of a magnitude to really provide benefit.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

While we agree with the concept of separating out monitoring and control we do see some possible confusion with the EACS and EAG definitions. We believe that there may be instances where a system or asset performs both functions. How would you classify and protect this device? Additionally, it appears from the chart above, “Proposed Requirements Related to EACMS Changes”, that all updated requirements for EACS and EAGs are applicable to the same requirements. For simplicity purposes, we suggest that EACS and EAG be combined into one definition: “Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

Likes 0

Dislikes 0

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT does not see a need to have a separate definition for EACS and EAG if they are both providing access control functions. The differentiation of controls is not of a magnitude to really provide benefit in separating the definitions. The concept should be incorporated into a single comprehensive definition along with CMS and EACS.

Likes 0

Dislikes 0

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support the proposed definition of EAG. EAPs may exist without an EAG. Reclamation recommends the SDT use existing industry-recognized terms to address the components of EACMS that control and authenticate electronic access, such as firewall, proxy server, router, etc.

If the SDT decides to use the proposed definition of EAG, Reclamation recommends the proposed EAG definition be changed

from: Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s). The Electronic Access Gateway also hosts the EAP(s)

to: Cyber Assets (including Electronic Access Points) that control electronic access to and from virtual and non-virtual Electronic Security Perimeter(s).

Reclamation also recommends the SDT change the definition of BES Cyber System as described in the recommended definitions section of the response to Question 24.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

While the definition of EAG further refines an approved, AEP requests the SDT refer to our response to Question #13.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

We can see some value from the proposed EAG definition but struggle in identifying how it supports security and reliability issues that are already addressed in the current Standards. The concern is adding EAG as another NERC Glossary Term will create unnecessary compliance and implementation complexity. When taken in total with all the proposed new and revised Glossary Terms and Requirements presented in this commenting form, the cumulative and gross effect is increased complexity with, likely, marginal improvement in security or reliability.

Alternative. If the SDT concludes the proposed definition is required to address the identified issues, an alternative approach is to remove electronic access control from the definition and include language that addresses the function of the EAG:

Electronic Access Gateway: Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s) the active function of filtering or forwarding traffic at the demarcation point (boundary protection). The Electronic Access Gateway also hosts the EAP(s).	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
We think that the SDT is attempting to differentiate hardware from virtual environment. The EAG hosts the EAP makes it seem that it is virtual. Some entities share a concern that the EACS and EAG are the same; is the EACS addressing lateral movement? Part 1.5 is applicable to EAPs for high & medium at control centers. With the new definition, will that no longer be applicable for EAPS? Is the BES Cyber Asset an EACS? Is it physical or virtual? Is the implication there that it is both? (for example: Domain controllers/TACACS) This creates an implementation challenge for entities given the dual nature of some devices. An Electronic Access Gateway hosts the EAP and performs the active function of filtering or forwarding traffic at the demarcation point (boundary protection). Primarily, these are firewalls and routers that perform gateway functions at the layer 3 ESP boundary demarcation point. Separation of duties issues here? The EAG hosts the EAP…makes it sound as if it is virtual. Internal discussions raised the question of whether the Electronic Access Gateway term is required.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	

Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Should be added as part of the EACMS definition.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Yes, as long as the concept of monitoring is also changed to solely be the classification of the monitoring data as BCSI, when applicable.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
The SDT used EAG Systems in the example for the changes to the BCSI definition. Public power is unsure if this should be EAG or EAGS.	
Likes 0	
Dislikes 0	
Response	

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
As stated in other comments, the SDT used EAG Systems in the example for the changes to the BCSI definition. I am unsure if this should be EAG or EAGS.	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	

16. Do you agree that the current compliance requirements related to EACMS monitoring systems are precluding or discouraging solutions that could reduce risk to security and reliability? Please provide your rationale in support or against this assertion.

John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
We feel all the requirements are reasonable as-is and would rather see consistency, even if the standard is increased.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The current EACMS parameters are sufficient in providing implementation structure and flexibility to ensure security and address the differences found in entities' system designs without highly prescriptive Requirements.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP agrees that the current requirements related to EACMS systems may preclude the optimal security and reliability solutions. AEP requests the SDT refer to our response to Question #13.	
Likes 0	
Dislikes 0	

Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ATC already treats our enterprise level monitoring systems as EACMS devices.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation supports the current compliance requirements related to EACMS. The Impact Rating Criteria provides the necessary clarity to reduce security and reliability risks. Reclamation recommends simplifying the Impact Rating Criteria in CIP-002 and changing the definition of BES Cyber System, as described in the recommended definitions section of the response to Question 24.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
no strong opinion	
Likes 0	
Dislikes 0	

Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
The current compliance requirements related to EACMS monitoring systems do not differentiate, preclude or discourage solutions that could reduce risk to security and reliability.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standard Review Group feels that the current compliance requirements give the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST has not encountered situations with its Bulk Electric System clients wherein an entity has avoided using security event monitoring and analysis systems due to concerns related to EACMS requirements.	
Likes 0	
Dislikes 0	

Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
We do not believe a change is necessary.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
The current compliance requirements related to EACMS monitoring systems do not differentiate, preclude or discourage solutions that could reduce risk to security and reliability.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
We have not encountered difficulty implementing enterprise grade security solutions with the current requirements.	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with this. See the same comments as in question 14.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
We believe that current compliance requirements may be hindering the use of cloud sourcing the SIEM function. We recommend consideration of removing the controls devices away from the BES Cyber Systems….can that be broken out of the applicability section? We also recommend separate controls for the electronic monitoring systems	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
Separating monitoring controls from EACMS definition reduces security posture.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	
City Light supports BPA's position and comments.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
We believe that current compliance requirements may hindering the use of cloud sourcing the SIEM. We recommend consideration of removing the controls devices away from the BES Cyber Systems….can that be broken out of the applicability section? We also recommend separate controls for the electronic monitoring systems.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	

Comment

Yes. The existing standards would make it difficult or maybe impossible to be compliant and use services like Dell Secureworks.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

ERCOT agrees that the current compliance requirements related to EACMS monitoring systems are precluding or discouraging solutions that could reduce risk to security and reliability. The current requirements are written to an asset level that requires the entities to be the ones managing the devices. With vendors going to more hosted service based solutions, the asset focus of the CIP requirements for EACMS pose serious problems when picking security solutions that provide more event correlation and expertise.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company agrees that the compliance burden currently placed on systems only used for electronic access monitoring and alarm response as per CIP-007-6 R4 are a hindrance to reaping the full security benefit of integrated SIEM systems. Southern supports the SDTs direction in this regard and agrees that the proper scoping of such systems as BCSI repositories is accurate.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	Yes
Document Name	
Comment	
We do agree that current requirements on EACMS that perform access monitoring discourage entities from using enterprise wide solutions that could, if in use, provide better visibility into trends and emerging threats.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
The current requirements are written to an asset level that requires the entities to be the ones managing the devices. With vendors going to more hosted service based solutions, the asset focus of the CIP requirements for EACMS pose serious problems when picking security solutions that provide more event correlation and expertise.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
The classification of monitoring systems as an EACMS currently limits the ability of utilizing enterprise solutions to provide this function. By eliminating this restriction a more enterprise wide approach can be evaluated to increase correlation and improve overall security monitoring.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	

Answer	Yes
Document Name	

Comment

Tacoma Power supports comments submitted by APPA.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

AZPS currently separates CIP monitoring systems from corporate monitoring systems and therefore, data analytics are impacted. With the SDT's proposal that the information contained within EACMS be protected as a BCSI repository, this would allow Responsible Entities to have more flexibility to incorporate data from multiple monitoring sources to better evaluate risks to security and reliability.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	Yes
Document Name	

Comment

Yes. The existing standards would make it difficult or potentially impossible to be compliant and use services like Dell Secureworks.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes

Document Name	
Comment	
Entities have made decisions based upon this compliance uncertainty in the past. Solutions that could reduce risk are hampered by this outdated model as noted by industry security advocates.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Yes. The existing standards would make it difficult or maybe impossible to be compliant and use services like Dell Secureworks.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA suggests security monitoring should be implemented in a manner that avoids any adverse operational impact on security event discovery and prevents introduction of a path that attackers could compromise to introduce malware.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Tools that provide great benefit by monitoring system events, performance and health often collect access information also, sometimes by default. These systems, not used as EACMS, are considered as such for regulatory purposes and that discourages the use of all but the most necessary tools.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	

Utilizing enterprise-wide monitoring and alerting systems may allow a better picture of a security threat.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
Entities are choosing to deploy a second monitoring solution (e.g., SIEM) for monitoring BCS only, in order to avoid expanding compliance obligations to enterprise systems. Due to the smaller scope of this second monitoring solution, the chosen application may be inferior to existing enterprise solutions to reduce costs. Additionally, the entity now loses the ability to correlate enterprise and BCS events, reducing the effectiveness of both monitoring solutions.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No Comment at this time.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

17. Should the security requirements for the access control portion of the EACMS to be different from the monitoring portion of the EACMS? If you do, please provide your rationale.

Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
These requirements should be the same.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
We raise the question: would it be problematic if we don't apply different access control standards? We recommend consideration that the requirements be expanded as noted in comments above to address gaps in standards/risks.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with this. See the same comments as in question 14.	
Likes 0	
Dislikes 0	
Response	

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

We believe that it is just as important to protect the monitoring systems as it is to protect the access control systems. Monitoring systems have extremely valuable information to attackers. They could even mask an attack if the monitoring system were compromised.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes that within the context of the existing CIP Standards, it is reasonable for the same set of security requirements to be applied to both access control and monitoring functions. Moreover, N&ST believes that trying to establish two different sets of requirements, one for each major function addressed by the existing definition of EACMS, could lead to confusion over how to identify and apply CIP-mandated controls to systems that perform both functions.

N&ST is strongly opposed to the idea of allowing systems that perform security event monitoring to be categorized as BSCI repositories rather than EACMS and disagrees with the assertion it would “result in improved security and reliability.” At the present time, systems acting as “designated storage locations” for BSCI and performing no other reliability function are not subject to any CIP requirements other than CIP-004 R4 and R5.

Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standard Review Group feels that the current compliance requirements give the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation supports the current definition of EACMS. Existing requirements that equally address access control and monitoring are adequately defined. The Impact Rating Criteria appropriately determines the protection each system requires.	

Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the current definition of EACMS allows for independent Cyber Assets to perform the separate functions as well as a combined function and that there is little to no difference in the risks presented. If the access control portion and the access monitoring portion can be separated, then yes security requirements for the access monitoring portion should be less restrictive (e.g. classifying the access monitoring portion as a BCSI repository).	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The EACMS access control and monitoring portions each play crucial roles protecting the security and reliability of the BES. Creating a dichotomy between the EACMS access control and monitoring requirements does not necessarily improve either and only creates added operational and compliance complexity.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

We raise the question: would it be problematic if we don't apply different access control standards? We recommend consideration that the requirements be expanded as noted in comments for Question 16 to address gaps in standards/risks.

Likes 0	
Dislikes 0	

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	Yes
Document Name	

Comment

The risks presented by the two types of systems are different. Compromise of the control portion gives the attacker immediate access to the systems being protected. Compromise of the monitoring portion may provide the attacker the ability to mask their actions and it may also provide them with information they can use to breach the control portion, but it does not grant them immediate access to the protected systems. The requirements should be different, but should take into account the risks posed by each system and address them appropriately.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

The ability to control access to essential systems carries a far greater risk than the ability to log events related to essential systems. Both should be protected, but the protections for access control systems should be held to the highest level feasible.

Likes 0

Dislikes 0

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	Yes
Document Name	

Comment

We agree with the SDT that the risk exposed by monitoring systems is lower than the risk exposed by access control systems.

Likes 0

Dislikes 0

Response

Bob Case - Black Hills Corporation - 1 - WECC

Answer	Yes
Document Name	

Comment

Monitoring systems should not have the same compliance regulations for BCS, so use of enterprise-wide systems can be utilized rather than discouraged.

Likes 0

Dislikes 0

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy agrees with the differentiation between access control and monitoring and the relative risk is different for monitoring and active control.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

TVA supports the SDT’s efforts to implement graduated levels of controls aligned with the functions executed by EACMS subsystems. Access control and access monitoring are separate security control functions, and consequently have different security requirements that should be considered separately. Access control systems inherently pose a greater risk if compromised than a monitoring system.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC

Answer	Yes
Document Name	

Comment

The security controls for monitoring do not need to be a rigid since the BES cannot be negatively impacted solely by a compromise of a monitoring system.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

BPA believes the option should be available based upon an entity’s assessment of different risks and controls specific to individual technology choices. Handling of log/monitoring information is different than control of access methodology.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	Yes
Document Name	

Comment

The security controls for monitoring need to be flexible. This is because the BES cannot be negatively impacted solely by a compromise of a monitoring system.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
As the SDT highlighted, there are different risks associated with both portions of the EACMS. The risk associated with the monitoring portion of the EACMS is information leakage, whereas the risk associated with the access control portion is unauthorized access to BES Cyber Systems and modifications of their operational parameters. Therefore, AZPS agrees that different security requirements should apply to different portion of the EACMS.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Yes, the current language drives entities to separate CIP and non-CIP monitoring environments, increasing costs and slowing adoption of better monitoring systems. Requiring CIP004-5 protections for EACMS allows for monitoring environment consolidation, deeper threat analysis, and quicker security event response times.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Access control has a direct impact on who can access the system and what they can do in the system, whereas monitoring is constrained to visibility to what is happening in the system (less risk on the monitoring side as it is typically read only).	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
We agree with the SDT assertions that these are only collecting information about the BCS and not necessary to the operations of the BCS.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	

We agree that there are differing risks based on the functionality of EACMS. The risk associated with monitoring access is greatly reduced compared to the risk of controlling access. If a system that controls access to a BES Cyber System or Asset is compromised, the real-time ability to operate or control the BES could be reduced or severed altogether. Conversely, if a system the monitor's access to a BES Cyber System or Asset is compromised, the real-time ability to operate or control the BES is not compromised. Therefore, we agree that the requirements for the access control portion of the EACMS should be different from the monitoring portion.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

ERCOT agrees with the SDT assertions that the access monitoring systems are only collecting information about the BCS and not necessary to the operations of the BCS. This distinction does support consideration as a repository of BES Cyber System Information.

Likes 0	
Dislikes 0	

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer	Yes
Document Name	

Comment

We agree with the SDTs rationale for differentiation between access control functions and monitoring functions and therefore support the proposed adjustments to the controls associated to EACS vs EAMS.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ

Answer	Yes
Document Name	

Comment

The security controls for monitoring do not need to be a rigid since the BES cannot be negatively impacted solely by a compromise of a monitoring system.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC

Answer	Yes
Document Name	

Comment

The systems logically lend themselves to be separated.

Likes 0	
Dislikes 0	

Response

John Tolo - Unisource - Tucson Electric Power Co. - 1

Answer	Yes
Document Name	

Comment

We feel all the requirements are reasonable as-is and would rather see consistency, even if the standard is increased. That said, out of all the categories being proposed, the access control and monitoring are the most disparate in security needs.

Likes 0	
Dislikes 0	

Response

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	Yes
Document Name	

Comment

City Light supports BPA position and comments.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	

Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	

18. Should CIP-011 Requirement R2 scope be expanded to include designated storage locations for access monitoring systems? If not, please provide rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light believes the existing BCSI definition does not need to be modified. It is sufficiently broad as written to include access monitoring information. Guidance or outreach might be provided to make this point clear, but, again, the existing definition is adequate as is.

Likes 0	
Dislikes 0	

Response

John Tolo - Unisource - Tucson Electric Power Co. - 1

Answer	No
Document Name	

Comment

Storage needs to be specifically addressed as part of the ESZ conversation or—even more realistic—as part of its own standard set. How do we treat NFS volumes in a shared environment?

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

The CIP-011 discussion on the SIEM (re-use and disposal) may be a separate concern; a recent FRCC workshop comment made by RE auditors put forth the concept that all BCAs contain BCSI; by addressing CIP-011 R2 have to protect the SIEM even if it was not identified as an EACMS. The scope might need to be reduced.

Likes 0	

Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
We believe the full magnitude of the impact to a change in definition has not fully been identified to provide substantive comments on expanding CIP-011 R2 to include designated storage locations for access monitoring systems.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the existing CIP-011 requirement R2 language is specific enough to allow responsible entities to assess the vulnerability of any storage location they have chosen for BCSI and understand the security controls that are needed in the event that the access-monitoring portion of an EACMS is classified as a BCSI repository.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	No
Document Name	
Comment	
Request clarification. Is this question asking about only hosted systems?	

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT does not agree with expanding CIP-011 R2 to include a all repositories of BCSI. The context of removing “monitoring” from the EACMS was to address information that may be with a third party. As such, the Responsible Entity cannot provide asset-level compliance evidence for a third part.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Comments: Seems unnecessarily prescriptive

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

BES Cyber System Information, whether stored in a “designated storage location for access monitoring systems” or stored in a “designated storage location for BES Cyber System Information”, is at its core BES Cyber System Information. Adding levels of BES Cyber System Information risk based on storage location will cause confusion within the industry and provides no reliability benefit.

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	No
Document Name	
Comment	
Monitoring systems if they store information with context, would be covered under existing CIP Requirements. If monitoring systems do not store information with context, then there is no risk.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standard Review Group feels that the current definition gives the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
While Duke Energy can support this in theory, we believe that if the drafting team is intending to include data storage that is already a part of the EACMS, that a method will need to be provided on how the data should be stored and tracked, prior to disposal of said data.	

Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
BCSI outside the entities environment should be dealt with in the CIP standards apart from the existing Requirement R2.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
This information does not pose sufficient risk to the BES to warrant additional protections.	
Likes 0	
Dislikes 0	

Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes it may be appropriate to extend the applicability of CIP-011 Requirement R2 to all so-called “designated storage locations” for BES Cyber System Information.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The scope of CIP-011 Requirement R2 should not be expanded and is sufficient as written.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with this. We opined that the access monitoring system should be part of EACMS rather than becoming a BCSI repository.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
Some auditors are already putting forth the concept that all BCAs contain BCSI; by addressing CIP-011 R2 have to protect the SIEM even if it was not identified as an EACMS. The scope might need to be reduced. Need to provide more clarificaiton and the security benefit on the definition of BCSI as it relates to various information. It is not all a the same risk level. Need to use words like "information uesful to plan a cyber attack? Simply useful, or does the information provide just about eveything you need.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	

Answer	Yes
Document Name	

Comment

Reclamation does not support additional requirements created in CIP-011. Reclamation recommends the required level of protection be determined for all systems based on each system’s impact rating as described in the recommended Impact Rating Criteria in the response to Question 24.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Yes – because there is current ambiguity in the “Applicable Systems” assigned to CIP-011-2 R2. The requirement currently states “Prior to the release for reuse (or R2.2 disposal) of applicable Cyber Assets”, which only includes High Impact BES Cyber Systems and Medium Impact BES Cyber Systems, and their associated EACMS, PACS, and PCAs; however, BCSI could reside in other places besides on those applicable systems. The requirement should be made clearer to direct the sanitization requirements to BCSI, regardless of where it resides, prior to the release for reuse or disposal.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

BPA believes that this should be a security objective, not a prescriptive technical requirement, and secure storage of SIEM information can be accomplished contractually. FedRAMP published guidance for outsourced storage services.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
To prevent leakage of BCSI.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	

Answer	Yes
Document Name	
Comment	
Yes – access monitoring systems can potentially contain BCSI and should be protected as such. That being said, monitoring systems also pose an additional risk that BCSI on its own does not: i.e. compromise of a monitoring system can be used to mask attempts to compromise the access control systems and the BCS itself. This additional risk needs to be addressed.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	
Document Name	

Comment

No comment at this time.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE does not have comments on this question.

Likes 0	
Dislikes 0	

Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
Yes.	
Likes 0	
Dislikes 0	
Response	

19. Do you agree with assignment of CIP Standard requirements to each of the EACS, EAG, and CMS categories as presented in the table above? If not, please provide rationale to support your position.

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

We believe that the table is incomplete and confusing by incorporate differnt concepts and definitions on the same table.

To address the splitting out of EACMS create table with:

- EACS, EAMS, and EACMS to clearly see what the diffrences would be

To address the new requirements for CMS and EAG place on a seperate table

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

We disagree with this. See the same comments as in question 14.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

Other than the requirement to segregate EACS systems into an Electronic Security Perimeter which is the whole point of this exercise, the requirements for EACS and EAG should be subsets of the existing EACMS requirements. The SDT should not be adding new requirements for these devices, such as CIP-009-6 R2.3 and CIP-010-2 R3.2, which do not currently apply to them.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

We do not believe a change is necessary.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST's "No" entry reflects "No" entries for questions 4, 14, and 15.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

CIP-004 R1.1 Awareness messages should not be limited by system type or function. All employees have a role to play in the BES security and should receive awareness.

CIP-004 R2 Cyber Security training should not be limited by system type of function.

CIP-004 R3.1 This requirement should not apply to EAGs as some work is done by a collection of analysts and reported on as a group such as a watch floor.

CIP-004 R3.4 Service providers should be able to provide evidence of their employee risk assessment process as an alternative to risk assessment conducted by the registered entity.

CIP-004 R4.2 CMS, EACS, EAGs should be able to show a process for granting and removing access, but a quarterly review should not be required.

CIP-004 R4.4 EACS & EAGs should not be labeled as BES Cyber System Information and a 15-month review should not be required.

CIP-004 R5.5 This should only apply to systems with ERC.

CIP-007, CIP-009, CIP-010, and CIP-011 should be modified to reflect the risk/impact of these systems to the BES.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS disagrees with the inclusion of CMS and EACS to the Applicable Systems of CIP-005 R1.x because both systems types may reside outside of an ESP and would not be applicable to R1.x.

AZPS proposes the addition of EACS to the Applicable Systems of CIP-005 R2.x because EACS responsible for authenticating Interactive Remote Access should be accessed through or be a part of an Intermediate System.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standard Review Group feels that the current definition gives the industry flexibility in this process. From our perspective, the proposed division of the definition will only cause confusion and put a huge burden on the industry to revise internal documentation as well as reclassifying their assets.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Xcel Energy believes CMS should also be included in CIP-009 R2.3. CIP-010 R3.2 has many questions around how it would be implemented and frequency of reviews, specifically for EACS.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	

- Awareness is not a good means of providing necessary content to SMEs managing these assets. The existing training requirements are more beneficial.
- The 36 month operational recovery exercise is limited to BES Cyber Systems and should remain with that scope.
- Recovery plans should be required for all assets other than PCA.
- See comments on question 18 regarding CIP-011 requirements.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

While we agree that many requirements will need to be updated based on the changes proposed in this comment form, there is some confusion on how the Applicable Systems will look based on the chart above. For instance, are the systems in the chart associated with high or medium impact BES Cyber Systems? Also, it is unclear how the CIP-005 Part 1 requirements will be applied to EACS. Furthermore, based on risk and current Applicable Systems, it is unclear what the justification is for adding EACS and EAGS to CIP-004 Part 1, CIP-009 Part 2.3 and CIP-010 Part 3.2 considering that EACMS are not currently part of the requirements.

Likes 0	
Dislikes 0	

Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Comments: Any CMS requirements need to be evaluated much more broadly than just in the context of virtualization. It doesn't make sense to singling out virtualization for special treatment that non-virtualized systems with similar risk-profiles do not get.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT does not agree with the assignments of the requirements as shown in the table. First, ERCOT does not see the need to define EACS, EAG, and CMS. With regards to the table, there are several concerns noted. (1) Awareness is not a good means of providing necessary content to SMEs managing these assets. The existing training requirements are more beneficial and appropriate. (2) The 36 month operational recovery exercise is limited to BES Cyber Systems. This should remain as the scope. (3) Recovery plans should be required for all assets other than PCA. This is the current requirement level. (4) See comments on question 18 regarding CIP-011 requirements.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
With the exception of CIP-002, Reclamation does not support modifying the existing standards.	

Reclamation recommends adding new or appropriate industry-recognized definitions to the NERC Glossary of Terms and revising the BES Cyber System definition as described in the recommended definitions section of the response to Question 24.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
The table does not provide enough detail to fully understand the compliance requirements for each Cyber Asset category. For example, does an EACS need to be in an ESP re: CIP-005 R1 Part 1.1?	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	No
Document Name	
Comment	
Since the question is about “access monitoring systems" it would include both electronic and physical access monitoring data. It is our view that not all monitoring data would need to be included since this information does not meet the BCSI definition.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	

AEP requests the SDT refer to our response to Question #13.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
SDG&E does not agree that CIP-005 2.3 could/should apply to CMS, EAGs and EACS if technically feasible.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The question is asking for support of the assignment of CIP Standards to proposed EACS, EAG, and CMS definitions in which we have concerns. We are unable to analyze the assignments with uncertainty around the definitions. We would note that the table illustrates how the proposed Glossary Terms—EACS, EAG, and CMS—potentially create more questions than clarity regarding compliance requirements and may present an undesirable effect of obscuring compliance obligations.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

We believe that the table is incomplete. Some redlines and comments are provided for the table itself. One example is to add to the CMS column for CIP-009. We recommend adding a column for EAMS since there is an option for the EACMS Glossary Term to be continued as it stands.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
Definitions are clear; the guidance is complex. Prefer consistency.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
The new categories of EACS, EAG, and CMS will be more descriptive and work better for the utilities as long as the definition of EACMS is retired. Combination of EACMS, EACS, EAG, and CMS may cause confusion and frustration for anyone trying to adequately define cyber assets into their proper category.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

N/A

Likes 0	
Dislikes 0	

Response

Bob Case - Black Hills Corporation - 1 - WECC

Answer	Yes
Document Name	

Comment

Conceptually, yes, but mapping table provided was not thoroughly vetted for this question.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC

Answer	Yes
Document Name	

Comment

There are requirements, specifically those found in R4 of CIP-007 about security event log retention and review. Does the SDT intend to have BCSI, designated storage location as the applicable systems for these requirements or remove these requirements for the monitoring systems altogether?

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	Yes
Document Name	

Comment

As long as the definition of CMS is modified as previously stated to scope it to virtual multi-instance environments.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
No. - Keep existing EACMS definition – do not create EAG and EACS.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
See comments in response to Question Nos. 13 – 17.	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	
Document Name	
Comment	
City Light is undecided at this time.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	

20. As the standards today do not prohibit the use of virtualization technologies, do you support an approach where no changes are made to the CIP Standards in response to the virtualization issue identified by the V5 TAG? Please provide a rationale to support your position.

Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light

Answer	No
Document Name	

Comment

City Light believes new approaches are necessary to accomodate virtualization with the CIP Standards, and generally supports the comments of APPA and BPA. City Light, however, would prefer the a more general cyber security approach be used for virtualization. NIST or PCI provide useful frameworks, rather than the VM Ware-centric approach proposed here.The VM Ware approach is not unreasonable, but aligns with a particular vendor.

Likes 0	
Dislikes 0	

Response

John Tolo - Unisource - Tucson Electric Power Co. - 1

Answer	No
Document Name	

Comment

Virtualization security needs to be addressed because security and operational gains are both important goals. We support addressing the concerns directly.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC

Answer	No
Document Name	

Comment

SDG&E contends that changes to the CIP standards must be implemented for virtualization in order to protect the integrity and safety of the Bulk Electric System as captured in our responses above.

Likes 0	

Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ

Answer	No
Document Name	

Comment

The current CIP standards do not explicitly prohibit all types of virtualization but require “high water marking” of the impact level even where this is not the most secure and reliable control. For example the separation of data plane and management plane between hypervisor and guest is a more effective control than applying high water mark CIP Requirements and keeping hypervisors inside the same security zone.

Also, CIP Requirements do not separate the electronic access controls from the electronic access monitoring to allow for different requirements when only monitoring is done. This has a high risk of misallocating scarce resources (money, time, manpower) that could be more effectively applied elsewhere for increased reliability.

Compliance Guidance is written to show one or more compliant solutions in order to clarify and help in applying the Requirements. It does not supersede Requirements language. The Guidance cannot show all possible solutions and is therefore inadequate because it is specific and limited, rather than a framework one can apply to generate new and unique solutions.   Solutions currently known to the SDT are only a snapshot in time that may become obsolete at any moment due to technical innovation or changes in the threat environment, while security objectives are more enduring than requirements for a specific solution. Entities may be aware of or devise a solution unknown to the SDT that provides equal or greater security but if the Requirements language doesn’t allow for the solution, it is not compliant. For these reasons, I think that the issues must be dealt with by revisions to the standards that emphasize security objectives and allow the Entity to demonstrate and explain how the solution meets the objective.

Likes 0	
Dislikes 0	

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer	No
Document Name	

Comment

ATC believes that there is merit to this concept; however, we answered “No” because guidance alone cannot solve the specific subject of virtualization due to the current construct of the CIP Requirements and its reliance on prescriptive controls that lean toward less advanced technological solutions. ATC could support ERO Enterprise-endorsed Compliance Guidance as an alternative if it were complimented by a paradigm shift to reshape the CIP Standards such that they are focused on technology agnostic security objectives and written with flexibility so Registered Entities are able to define and implement an adaptive risk-based cybersecurity program that timely detects, responds to, and mitigates emerging threats. ATC welcomes thought leadership on the subject of ERO Enterprise-endorsed Compliance Guidance as an alternative to mandatory regulations to position the industry

for a more nimble, sustainable, and mature security posture. While there has been improvement in the requirement language as the CIP Standards have evolved, they continue to suffer because prescriptive mandatory regulations cannot keep pace with emerging technologies and the rapidly changing cybersecurity threat landscape. Until this paradigm shift occurs, the industry will continue to face the unintended consequences of the current construct, be distracted by the conundrum, divided between security and compliance, limited in our ability to leverage advances in technology, and will continue to be hindered by the antiquated ideals of a regulation that is chasing cybersecurity.

Likes 0	
Dislikes 0	

Response
Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment
With the exception of CIP-002, Reclamation does not support modifying the existing standards. Reclamation recommends that simplifying the Impact Rating Criteria in CIP-002 and adding new or appropriate industry-recognized definitions to the NERC Glossary of Terms to address virtualization technologies will resolve industry concerns (refer to the recommended definitions and revised Impact Rating Criteria sections of the response to Question 24).

Likes 0	
Dislikes 0	

Response
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment
Even though the requirements today do not prohibit the use of virtualization, the implementation of virtualization in today's CIP regulatory construct discourages an entity from realizing the full potential of virtualization. Making the right changes to the requirements will allow entities the ability to fully utilize emerging technologies while supporting the reliable operations of the BES.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
More definition is needed around virtualization. There is too much risk to the utility as it is left up to interpretation.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA. Tacoma Power supports comments submitted by BPA.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
The SDT should explicitly address virtualization in the CIP Standard to provide clarity for securely separating CIP assets in virtualized environments.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	

Answer	No
Document Name	

Comment

The current CIP standards do not explicitly prohibit all types of virtualization but require “high water marking” of the impact level even where this is not the most secure and reliable control. For example, the separation of data plane and management plane between hypervisor and guest is a more effective control than applying rigorous CIP Requirements and keeping hypervisors inside the same security zone.

Also, CIP Requirements do not separate the electronic access controls from the electronic access monitoring to allow for different requirements when only monitoring is done. This has a high risk of misallocating scarce resources (money, time, manpower) that could be more effectively applied elsewhere for increased reliability.

Compliance guidance is written to show one or more compliant solutions to clarify and help in applying the Requirements. Such guidance does not supersede standard requirements language. Moreover, such guidance cannot show all possible solutions and is specific and limited, rather than a framework where one can generate new and unique solutions. Solutions currently known to the SDT are only a snapshot in time that may become obsolete at any moment due to technical innovation or changes in the threat environment, while security objectives are more enduring than requirements for a specific solution. Entities may be aware of, or devise a solution unknown to the SDT that provides equal or greater security, that the Requirements language finds the solution non-compliant. Therefore, the proposed standard must emphasize security objectives that allow entities to demonstrate and explain how solutions meets the objective.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA believes that changes to the standards language are required to enable virtualization in a secure and reliable manner and that implementation should allow for secure shared infrastructure.

The NERC CIP SDT has a responsibility to evolve the standards language with our industry and not restrict its progress in adopting new, more efficient, fiscally responsible, secure, and reliable technology solutions. The current CIP reliability standards, as written, are not easily applied to new technologies, such as virtualization. They are written specific to dated industrial control systems of our industry and do not address virtualization technologies. If NERC uses only guidance rather than security objectives standards language, we can expect significant impacts, such as compliance violations, costly rework of in-flight and future planned upgrade projects, and slowing the adoption of new technologies that can better secure and improve the reliability of the Bulk Electric System.

- Guidance outside of the standards does not address the V5TAG mandate from the SAR to address virtualization in the standards language
- Without direct guidance in standards, entities can find themselves at risk of compliance violations due to individual different interpretations.
- It is clear from the debate regarding virtualization implementations that there is no universal agreement about shared infrastructure being allowed.

- Virtual Technology that is already in the near-term pipeline and deployed in other industries would benefit the energy industry.
- Without transitioning to a security objective-based standard, flexibility to adapt to new technology is lost.
- Presidential directives for government agencies already require aggressive moves to cloud computing for reasons of common secure platforms, scalability and cost benefit.

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC

Answer	No
Document Name	

Comment

The current CIP standards do not explicitly prohibit all types of virtualization but require “high water marking” of the impact level even where this is not the most secure and reliable control. For example the separation of data plane and management plane between hypervisor and guest is a more effective control than applying high water mark CIP Requirements and keeping hypervisors inside the same security zone.

Also, CIP Requirements do not separate the electronic access controls from the electronic access monitoring to allow for different requirements when only monitoring is done. This has a high risk of misallocating scarce resources (money, time, manpower) that could be more effectively applied elsewhere for increased reliability.

Compliance Guidance is written to show one or more compliant solutions in order to clarify and help in applying the Requirements. It does not supersede Requirements language. The Guidance cannot show all possible solutions and is therefore inadequate because it is specific and limited, rather than a framework one can apply to generate new and unique solutions. Solutions currently known to the SDT are only a snapshot in time that may become obsolete at any moment due to technical innovation or changes in the threat environment, while security objectives are more enduring than requirements for a specific solution. Entities may be aware of or devise a solution unknown to the SDT that provides equal or greater security but if the Requirements language doesn’t allow for the solution, it is not compliant. For these reasons, I think that the issues must be dealt with by revisions to the standards that emphasize security objectives and allow the Entity to demonstrate and explain how the solution meets the objective.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

To properly apply the standards to a virtual environment, they must be changed to adequately enforce the required security practices.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes would be appropriate to modify the CIP Standards in order to both clarify the applicability of requirements to virtual devices and, in some instances, to define new requirements (such as for ESZs) that would apply to virtual devices.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Cowlitz supports APPA comment.	

Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	No
Document Name	
Comment	
We support changes being explicit.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
The current CIP reliability standards as written are far too open to interpretation and not easily applied to new technologies, such as virtualization. New or modified CIP Standards surrounding virtualization will bring clarity and objective criteria to evaluate against such implementations.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
The current Cyber Asset doesn't clearly state that the programmable device includes virtual machine. Also current EACMS definition doesn't include the cyber system that can alter the configuration of BCS explicitly even though it implies that. As long as these definitions are modified, all applicable virtual devices would be protected by the current CIP standards.	

Likes 0	
Dislikes 0	

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	No
Document Name	

Comment

Currently, the standards require a bit of “common sense” interpretation to be applied to virtualized systems appropriately. Different entities may have different interpretations, some of which may not result in an appropriate level of security for the relevant BCS. Providing guidance may help in this regard, but adjusting the standards to address virtualization will ensure that a minimum enforceable level of security is applied by all entities without relying on interpretation.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

We agree with an approach that does not change the standards. We also recommend that the GTB should go into the Compliance Guidelines. We also recommend that the SDT yay just need to modify the definition of Cyber Asset.

There is a concern that the number of unanticipated consequences could be much more damaging than anything we are fixing with changes to the requirement parts and glossary terms. .

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI & Member G&Ts

Answer	Yes
Document Name	

Comment

The current CIP standards can apply to a virtual environment. Some guidance and examples would assist Registered Entities in identifying a compliant approach when implementing virtualization technologies. More specifically, ERO Enterprise-endorsed Compliance Guidance could be used to address the implementation of virtualization.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	Yes
Document Name	

Comment

KCP&L supports using current CIP Standards to address risk posed by virtualization.

Complexity Defeats Security

Some of the offered concepts may have merit but when considered independently or in total, the consequence of implementing and managing the proposed idea will assuredly add significant complexity to already complex systems.

By most any measure, complexity defeats security through obfuscation of vulnerabilities and can provide a false sense of security.

Promotes Flexibility. Virtualization technology will continue to evolve at a rate faster than the Standards can address. Compliance guidance provides a path for implementation and the Standards' role to be objective. Additionally, compliance guidance allows the flexibility to relieve compliance burdens on entities choosing not to implement virtual technologies.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	Yes
Document Name	

Comment

AEP believes a reasonable person can apply the existing CIP requirements in a virtual environment. A reasonable audit approach is possible as well. Implementation (Compliance) Guidance would be helpful.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

ERCOT agrees with making no revisions to the standards as proposed. See comments provided in response to questions 1-12. The concepts of virtualization have been contemplated since CIP version 1 requirements. Example implementations would be very beneficial to industry and suffice to provide the clarity needed irrespective of the technology implemented.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Given the current regulatory landscape and massive compliance challenges recently with evolving CIP Standards, Southern Company would be open to exploring, given the appropriate level of industry input and acceptance, ERO Enterprise-endorsed Compliance Guidance to address the proper implementation of virtualization.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	Yes
Document Name	

Comment

Comments: There are so many CMS-like systems that don't involve virtualization that singling out virtualization seems counterproductive. Certainly there is benefit to guidance as to how host systems/hypervisors are treated, but the guest systems seem to be straight-forward with regard to relevant controls.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.

Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Rather than changing the requirements, Texas RE suggests modifying the definition of Cyber Asset to also specifically include virtual devices. Virtual devices should be handled the same as physical Cyber Assets. Texas RE is concerned the proposed changes to the requirement language by the SDT appear too prescriptive.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
The current CIP standards, allow for virtual environments as CIP assets. Adding the changes above will make it more complex and add more confusion to the environments.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	Yes
Document Name	
Comment	
See comment #23.	
Likes 0	

Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CenterPoint Energy believes the current CIP standards can apply to a virtual environment. Some guidance and examples for workable solutions for hosted systems, virtual LANs, and even cloud based systems could help Registered Entities be more comfortable with their compliance approach when implementing virtualization technologies.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	Yes
Document Name	

Comment

All cyber assets in support of the BES should be afforded the highest level of protections as the highest watermark to reduce/mitigate any potential risks that can impact the systems directly or indirectly.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

Virtualization is not prohibited by the present version of the CIP Standards. Each hardware platform is considered a device and each VM running on the hardware is considered software and data on the device. This means that the hardware device and each VM running on that device must be protected at the level of the highest-impact VM running on the device. This is seldom an issue in a Control Center, where all Cyber Assets are protected at the level of the “high-water-mark.”

Economic considerations seem to be the biggest driving force in pushing forward “mixed-trust” virtual systems. These considerations will primarily benefit relatively the relatively few companies that can justify the large-scale systems needed for a significant economic return. Other companies will be required to wade through a number of new requirements that may have little benefit to them.

In addition, properly securing mixed-trust virtual systems requires a staff with substantial skills and training. The staff of mid-size and small companies may be ill-equipment to succeed in that endeavor.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	Yes
Document Name	

Comment

We agree with an approach that does not change the standards. We also recommend that the GTB should go into the Compliance Guidelines. We also recommend that the SDT may just need to modify the definition of Cyber Asset.

There is a concern that the number of unanticipated consequences could be much more damaging than anything we are fixing with changes to the requirement parts and glossary terms.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	

Answer	
Document Name	
Comment	
No. Keep standards up to date with existing technologies else future revisions will take tremendous time to be developed.	
Likes 0	
Dislikes 0	
Response	

21. Is your organization in support of Concept 1: Modifications to allow use of secure multi-instance? Please provide rationale to support your position.	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	No
Document Name	
Comment	
Maybe If the changes were made per the comments above, we might be able to support the concept. If there are no changes made related to concept 1, we do not support it.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Modifications to allow the secure use of multi-instance will add a large amount of complexity and ambiguity to the CIP Standards while providing a significant benefit to only a small number of entities.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We never use multi-instance concept. It is not clear whether it only applies to the virtual machines or physical devices as well.	
Likes 0	
Dislikes 0	

Response

Bob Case - Black Hills Corporation - 1 - WECC

Answer	No
Document Name	

Comment

Modifications are not required for secure multi-instance environments. What the SDT is proposing is secure, and non-secure, multi-instance environments. We support exploring how multi-instance environments could be allowed in a secure manner, but this appears to be a change to save costs, not necessarily increase security.

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA

Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx

Comment

Please see attached comments

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

Unless properly designed, configured and implemented multi-instance environments can lead to potential unknown/unrealized risks, added complexity, and added compliance exposure for systems not associated with BCA's. Segregated environments can be more beneficial in reducing overall risk and compliance exposure.

Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
See comments in response to Question Nos. 1-12.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Our position is that it would be difficult to secure a multi-instance environment and difficult to audit and thus too much risk to BES Cyber Systems to be utilized.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
See comments to questions (1 – 12) referencing the Concept 1 Section.	
Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Xcel Energy believes that further development of concepts and terms is needed before support can be given to any of the proposed options.	
Likes 0	
Dislikes 0	
Response	

David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	
See comments provided in response to each question under Concept 1.	
Likes 0	
Dislikes 0	
Response	

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
Unless properly designed, configured and implemented multi-instance environments can lead to potential unknown/unrealized risks, added complexity, and added compliance exposure for systems not associated with BCA's. Segregated environments can be more beneficial in reducing overall risk and compliance exposure.	
Likes 0	
Dislikes 0	
Response	

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
While we are in support of the modifications to allow the use of secure multi-instance we have some concerns, questions and suggestions on the current approach. Please see our comment on question 24.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Comments: Clarity should be provided on the equivalence between virtual cyber assets and physical cyber assets. Systems involving multiple cyber assets (physical or virtual), or centralized management systems (VMs, SDNs, SANS, Antivirus, etc.), should be addressed as a whole in a risk-based way. Virtualization should not be singled out for special scrutiny.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	No
Document Name	
Comment	
The concepts and definitions proposed need additional clarification to ensure proper scoping and applicability of any subsequent requirements. Southern appreciates the SDTs work in this regard, and views this as a step in the right direction, but additional refinement appears to be needed.	
Likes 0	
Dislikes 0	

Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
See comments provided in response to questions 1-12.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
With the exception of CIP-002, Reclamation does not support modifying the existing standards. Reclamation recommends that simplifying the Impact Rating Criteria in CIP-002 and adding new or appropriate industry-recognized definitions, including Virtual Instance and Multi-Virtual Instance, to the NERC Glossary of Terms to address the use of secure multi-instance (refer to the responses to Questions 6 and 24).	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the existing RS requirement language and the definition language with minor modifications is sufficient.	
Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC

Answer	No
Document Name	

Comment

SDG&E seeks resolution to comments posted regarding Concept 1 before it moves forward.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	No
Document Name	

Comment

Modifying the Requirements to allow use of secure multi-instance is not necessary. Entities require flexibility to address the spectrum of systems within the entity and external to the entity. Adding Requirements unfavorably impacts the desired flexibility implementing Standards and managing the security of Cyber Systems.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

In virtualization terminology, “instance” is used to describe a single *instance* of a resource. If the SDT means “multi-tenant” in their use of “multi-instance”, it is suggested to use the former term. It is easier to explain that an organization can internally have many “tenants” that for whom shared resources are compartmentalized then to explain having multiple instances of environments which in turn have multiple instances of computing resources. It’s difficult to communicate about compliance and virtualization even amongst people who understand the distinction between the two types of instances.

The CMS is a good approach. It would be preferable to only be applicable to Virtualized Systems, at least at first, in effort to address the systemic risk introduced by virtualization.

The ESZ concept does not reflect how virtualization systems work and adds an extra level of unnecessary and confusing complexity to the CIP standards. What is needed is requirements that, if met, let virtual cyber assets be treated as “normal” cyber assets. And similarly, virtual networks the same as “normal” physical networks. Then the existing body of CIP Standards can be leveraged to mitigate additional virtualization risks without adding undo complexity and exceptions.

Suggest requirements to the effect of:

> Virtualization host environments must have mechanisms to ensure virtual machines or virtual components of machines (compute, network interface, storage) utilize mechanisms to ensure they are unable to interact with each other except as necessitated by design to fulfill their function. Ie: no direct compute node to compute node interaction, storage node to storage node interaction. Compute nodes can only access the storage resources they are specifically assigned. Virtual network interfaces are constrained to one virtual network (VLAN). Etc. The specific interaction being allowed and the details how this is enforced must be documented (IE VLAN#, etc).
>
> Possibly a requirement to test that the configuration needed for above requirement correctly isolates/segregates virtual resources (again, only for virtualization).
>
> CMS used for managing virtualization hosts (ie. the management plane) must reside in a ESP that is distinct from the ESP of the virtual cyber assets it hosts (which still allows, incidentally, self hosting of management virtual machines)

Likes 0	
Dislikes 0	

Response

Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

Maybe

If the changes were made per the comments above, we might be able to support the concept. If there are no changes made related to concept 1, we do not support it.

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	Yes
Document Name	

Comment

The current version fo the standard is too open for individual interpretation. The effort to provide consistency is welcome.

Likes 0	
Dislikes 0	

Response

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	Yes
Document Name	

Comment

In general this concept addresses virtualization in a more consistent manner and avoids reliance on individual entities' interpretation. There may be areas which can be improved, but in general this is a step in the right direction.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	Yes
Document Name	

Comment	
While we generally support the approach outlined in Concept 1, it requires further refinement and needs to be explicitly drafted to truly understand the ramifications of the changes proposed. The current form is unacceptable, and needs revision Additionally, the concept addresses storage in its explanation, but does not address it in the requirements and definitions.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST believes would be appropriate to modify the CIP Standards in order to both clarify the applicability of requirements to virtual devices and, in some instances, to define new requirements (such as for ESZs) that would apply to virtual devices.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	

Comment	
Properly implemented security controls, monitoring, and processes can afford protections of a multi-instance virtual environment.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Lack of language addressing virtualization leaves significant risk of misunderstanding between auditors and entities on proper implementation of multi-instance infrastructure. The problem of auditors and entities interpreting current standards applied to virtual implementations differently exists already even when using virtualization in a single-instance environment.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Yes, provided that comments herein, are taken into consideration.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
AZPS is a proponent of virtualization, but wants to do so in a safe and reliant manner. The allowed use of multi-instance environments would help to maximize resources and minimize costs.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
Virtual architecture is important and must be directly addressed. If no regulations occur, we will still apply a high standard of security to these systems.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	
Comment	

City Light supports the comments of APPA and BPA, but encourages continued careful development, modification, and clarification of the concepts before they become enforceable Standards.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Lauren Price - ATCO Electric - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
Yes.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	

Document Name

Comment

The ISO supports the comments of the Security Working Group (SWG)

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE suggests the current definitions and requirements are sufficient to protect virtual devices as virtual devices should be afforded the same protection as physical devices.

Likes 0

Dislikes 0

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer

Document Name

Comment

No comment at this time.

Likes 0

Dislikes 0

Response

22. Is your organization in support of Concept 2: Modifications to the EACMS definition? Please provide rationale to support your position.	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	No
Document Name	
Comment	
We prefer consistency to the compliance complexity of dividing the roles into three and tracking requirements separately.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Industry could support it if it allowed entities to use cloud based SIEM. If it does not allow for cloud based SIEM support, they need to modified. This introduces more complexity and ambiguity due to unanticipated consequences	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The current EACMS elements are sufficient in providing implementation structure and flexibility to ensure the differences found in entities' system designs address security without requiring highly prescriptive Standards.	
Likes 0	
Dislikes 0	
Response	

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	
SDG&E seeks resolution to comments posted regarding Concept 2 before it moves forward.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP agrees there is value in EACMS definition to allow the access-monitoring portion of the EACMS to be reclassified as a BSCI repository and the introduction of the CMD definitions, but does not support the additional definitions. We also believe that a revised definition of EACMS is all that is necessary to address the concerns.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
With the exception of CIP-002, Reclamation does not support modifying the existing standards. Reclamation recommends that simplifying the Impact Rating Criteria in CIP-002 and adding new or appropriate industry-recognized definitions to the NERC Glossary of Terms will resolve industry concerns (refer to the recommended definitions section of the response to Question 24).	
Likes 0	
Dislikes 0	

Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT recognizes the value and supports only the changes related to monitoring systems. See comments provided for questions 13-19.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	
See comments provided in response to each question under Concept 2. Other than the monitoring part.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Xcel Energy believes that further development of concepts and terms is needed before support can be given to any of the proposed options. Further granularity around 3rd party/off the shelf software would be helpful.	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
The SPP Standard Review Group feels that the drafting team has potentially added complexity to the process with the proposed language as well as an additional burden for the process to be implemented.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes modifications are not necessary and notes further that the so-called “hall of mirrors” problem that is put forth as a possible reason to modify the EACMS definition is not an inherent problem in either the existing EACMS definition or the current applicable CIP requirements.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
See comments in response to Question Nos. 13-19.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	

Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	
Comment	
While the idea of splitting the definition of EACMS to allow broader implementation of security controls is appealing, that does not appear to be what the SDT is proposing. The SDT does remove most requirements for EAMS, but ramps up the requirements on EACS and EAG. For entities who have already implemented a SIEM in their CIP environment, there is little benefit, as we have already borne the burden of implementing CIP on our SIEM. While declassification might remove some of the burden, it is far outweighed by the increased obligation proposed by the SDT.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with the modification to the EACMS definition and we proposed a different way to modify the EACMS definition (see question 4 feedback).	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	

Answer	No
Document Name	

Comment

Industry could support it if it allowed entities to use cloud based SIEM. If it does not allow for cloud based SIEM support, they need to modified. This introduces more complexity and ambiguity due to unanticipated consequences

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company agrees with the SDT that the current construct of the EACMS definition and associated requirements does not differentiate controls based on the functionality and risk of the system. Southern Company supports the SDTs efforts to address this by breaking up the EACMS categorization of applicable systems by function so that the appropriate requirements for each can be applied.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	Yes
Document Name	

Comment

Comments: In general, we agree with the rationale provided.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	Yes
Document Name	

Comment

We are in support of the concept to modify the EACMS definition. The current definition does not take in account the types of assets contained with the EACMS definition and the risk of each type of asset.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

To be more inclusive and defined.

Likes 0	
Dislikes 0	

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	Yes
Document Name	

Comment

Tacoma Power supports comments submitted by APPA.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	
Comment	
The proposed modifications will increase the visibility for monitoring of CIP and other unrelated systems, but should be provided with an additional thorough evaluation to ensure that no unintended gaps or consequences could result as discussed above.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	Yes
Document Name	
Comment	
Yes, provided that comments herein, are taken into consideration.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The term EACMS is too broad and not well defined. It does not address actual risk or available technical controls.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	

Answer	Yes
Document Name	
Comment	
TVA welcomes the distinctions allowed by the modification to the EACMS definition. Changing the definition and revising the applicable standards will allow utilities to better protect the BES, and reduce the compliance burden on these systems.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
To be more inclusive and defined	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz supports BPA comment.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	

Comment	
Provided the goal is to promote using enterprise wide monitoring systems to monitor BCS.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
The proposed changes will permit entities to protect electronic access control systems commensurate with the risk of those systems to the BES.	
Likes 0	
Dislikes 0	
Response	
Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5	
Answer	Yes
Document Name	
Comment	
We support the new definition of EACS, EAG, and CMS, so long as EACMS is retired. This concept allows for improved use of enterprise monitoring solutions which should lead to better risk mitigation. However, only applying the BCSI requirements to monitoring solutions may not sufficiently address the risk that a compromised monitoring solution could be used to mask additional attacks. This additional risk needs to be addressed appropriately.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response
Lauren Price - ATCO Electric - 1 - MRO,RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE suggests the current definitions and requirements are sufficient to protect virtual devices as virtual devices should be afforded the same protection as physical devices.	
Likes 0	

Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
No. Existing EACMS definition provides adequate security controls to access control systems and monitoring systems.	
Likes 0	
Dislikes 0	
Response	

23. Is your organization in support of Concept 3: Compliance Guidance? Please provide rationale to support your position.

Joel Charlebois - AESI - Acumen Engineered Solutions International Inc. - 5

Answer	No
Document Name	

Comment

Relying on guidance allows for too much interpretation on behalf of the entities and may lead to an inconsistent level of security between entities. In addition, implementation guidance is just as the name suggest, guidance, and is meant to describe one or more methods of being compliant, but is not meant to be the only method to be compliant. An entity is free to choose an alternative implementation that is not described by implementation guidance, and wether or not that alternative implementation is compliant is still subject to interpretation.

Adjusting the standards instead of just providing guidance should ensure correct and consistent interpretation of requirements across the industry, while providing entities with sufficient assurance that their methods of implementation are compliant.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

The current CIP reliability standards as written are far too open to interpretation and not easily applied to new technologies, such as virtualization. New or modified CIP Standards surrounding virtualization will bring clarity and objective criteria to evaluate against such implementations.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	No
Document Name	

Comment

No answer supports previous comment above.

Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5,6 - FRCC, Group Name FMPA	
Answer	No
Document Name	2016-02_Virtualization_Unofficial Comment Form_FMPA_comments.docx
Comment	
Please see attached comments	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST considers Compliance Guidance on various topics an important and useful tool, and would support the creation and dissemination of guidance that addresses some of the myriad security and compliance issues that may be associated with the use of virtual technology. However, N&ST does not consider it an adequate substitute for modified CIP Standards that clarify the applicability of requirements to virtual environments.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The language of the standard should address the use of virtualization technologies. Compliance guidance is insufficient to address the issues that have been identified.	

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC

Answer	No
Document Name	

Comment

No. Compliance Guidance would not be appropriate because it only shows one or more methods of compliance and not all. It also does not resolve the issues of high-water marking of impact levels and allow for the separation of monitoring from EACMS.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA strongly believes that standard language is necessary for all facets of virtualization. See response to question 20 above.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	No
Document Name	

Comment

APPA believes that the Compliance Guidance would not be appropriate because it only shows limited compliance. Moreover, it does not resolve the issues of high-water marking of impact levels and nor does it allow for the separation of monitoring from EACMS.

Likes 0	

Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
The SDT should explicitly address virtualization in the CIP Standard to provide clarity for securely separating CIP assets in virtualized environments.	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma Power supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy agrees that Compliance Guidance is helpful to industry for understanding and implementation, however, we request further clarification on whether industry stakeholders will be provided an opportunity to comment on any compliance guidance that is drafted, and ultimately approved by NERC.	
Likes 0	

Dislikes 0

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

The CIP Standards doesn’t currently allow mixed trust in the virtual environment. From our perspective, this will require changes to CIP Standards to help implement virtualization technologies and have a positive impact on the industry.

Likes 0

Dislikes 0

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE

Answer	No
Document Name	

Comment

Xcel Energy believes that further development of concepts and terms is needed before support can be given to any of the proposed options.

Likes 0

Dislikes 0

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

Even though the requirements today do not prohibit the use of virtualization, the Compliance Guidance and the current requirements discourages an entity from realizing the full potential of virtualization. Making the right changes to the requirements will allow entities the ability to fully utilize emerging technologies while supporting the reliable operations of the BES.

Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation does not support the use of separate Compliance Guidance documents. Reclamation recommends that existing standards be revised with sufficient clarity to endure changing technologies and provide necessary guidance within the requirements and measures. Reclamation also recommends that adding new or appropriate industry-recognized definitions to the NERC Glossary of Terms will resolve industry concerns with the implementation of virtualization (refer to the recommended definitions section of the response to Question 24).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ	
Answer	No
Document Name	
Comment	
No. Compliance Guidance would not be appropriate because it only shows one or more methods of compliance and not all. It also does not resolve the issues of high-water marking of impact levels and allow for the separation of monitoring from EACMS.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8,9 - WECC	
Answer	No
Document Name	
Comment	

SDG&E seeks resolution to comments posted regarding Concept 3 before it moves forward.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
This could be resolved by improving the definition of Cyber Asset. Given that Compliance Guidance is for the auditors without input from industry, there would be no need for changes if no changes are made to the standards. Implementation Guidance on virtualization infrastructure would be beneficial.	
Likes 0	
Dislikes 0	
Response	
Paul Haase - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light	
Answer	No
Document Name	
Comment	
City Light supports the positions and comments of APPA and BPA.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
This could be resolved by improving the definition of Cyber Asset. Given that Compliance Guidance is for the auditors without input from industry, there would be no need for changes if no changes are made to the standards. Implementation Guidance on virtualization infrastructure would be beneficial.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Using Implementation Guidance, and CMEP Practice Guides if necessary, to clarify the permitted uses of virtual systems in a CIP environment should reduce an entity's uncertainty about employing such systems.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
We support this compliance guidance since it explains what constitutes a programmable device.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Having it defined is better than not having it detailed and explained.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
More guidance affords greater understanding and clearer interpretations.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

See comments in response to Question No. 20.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	Yes
Document Name	
Comment	
The current standard is sufficient; there is no need to change it. We think that guidance helping entities better understand the intent of the standard and how to be compliant is good. Regional Entities have written Standard Application Guides to assist with this very issue.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
More guidance affords greater understanding and clearer interpretations.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Given the current regulatory landscape and massive compliance challenges recently with evolving CIP Standards, Southern Company would be open to exploring, given the appropriate level of industry input and acceptance, ERO Enterprise-endorsed Compliance Guidance to address the proper implementation of virtualization. However, if pursued, Compliance Guidance should be accompanied by the changes to the Standards proposed in Concept 2 to differentiate controls based on the functionality and risk of current EACMS systems.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

ERCOT asserts that ERO-endorsed implementation guidance would be the most appropriate means to address the various mean of implementing virtual technologies. See comments provided in response to question 20.

Likes 0	
Dislikes 0	

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer	Yes
Document Name	

Comment

ATC supports the concept of Compliance Guidance. That said, where the requirements are written in a prescriptive manner such that the guidance is at odds with the requirements, Registered Entities cannot leverage that guidance without risking non-compliance. This condition renders even the soundest guidance unusable. ATC could support ERO Enterprise-endorsed Compliance Guidance as an alternative if it were complimented by a paradigm shift to reshape the CIP Standards such that they are focused on technology agnostic security objectives and written with flexibility so Registered Entities are able to define and implement an adaptive risk-based cybersecurity program that timely detects, responds to, and mitigates emerging threats. ATC welcomes thought leadership on the subject of ERO Enterprise-endorsed Compliance Guidance as an alternative to mandatory regulations to position the industry for a more nimble, sustainable, and mature security posture. While there has been improvement in the requirement language as the CIP Standards have evolved, they continue to suffer because prescriptive mandatory regulations cannot keep pace with emerging technologies and the rapidly changing cybersecurity threat landscape. Until this paradigm shift occurs, the industry will continue to face the unintended consequences of the current construct, be distracted by the conundrum, divided between security and compliance, limited in our ability to leverage advances in technology, and will continue to be hindered by the antiquated ideals of a regulation that is chasing cybersecurity.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	Yes
Document Name	

Comment

AEP believes Implementation (Compliance) guidance is important to provide industry, auditors and regulators sufficient insight into the concepts of virtualization and how the existing requirements are applicable in a virtual environment. We also agree that modifications are needed to the CIP standards along with additional compliance guidance.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	Yes
Document Name	

Comment

Compliance guidance that informs “a way” for compliance has value. Guidance establishing compliance thresholds, bright-line requirements, incents entities to meet only the minimum compliance threshold and inhibits viewing compliance through a risk lens.

The optimal guidance provides entities ideas and the flexibility to address identified risks.

Likes 0	
Dislikes 0	

Response

John Tolo - Unisource - Tucson Electric Power Co. - 1

Answer	Yes
Document Name	

Comment

With caveats listed in-section.

Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	
The current CIP standards can apply to a virtual environment. Some guidance and examples would assist Registered Entities in identifying a compliant approach when implementing virtualization technologies. More specifically, ERO Enterprise-endorsed Compliance Guidance could be used to address the implementation of virtualization.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	2016-02_Virtualization_Unofficial Comment Form_11022017.docx
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
Yes.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	
Texas RE suggests the current definitions and requirements are sufficient to protect virtual devices as virtual devices should be afforded the same protection as physical devices.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	

24. If you have additional comments that you have not provided in response to the questions above, please provide them here.

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
No comment at this time.	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	
Document Name	
Comment	
We are confused about VLANs. The current guidance has been to avoid VLANs, ostensibly over concerns that their “software-based nature” is somewhat insecure. We don’t disagree that they are “less secure” than physical LANs, however we believe they have a place within the environment to separate CIP and NON-CIP assets as they traverse into the firewall. This allows us a multi-instance network environment as opposed to dedicated network hardware for CIP. This confusion arises because software-derived separations for the server-side of multi-instance environments seems to be your specific intent. In summary, NSX to separate VMs is acceptable but VLANs to separate networks is not. That seems inconsistent to us. In fact, VLANs have well-known ways in which to secure them while products like NSX are much less well-known and proven. We would view VLANs as a good way to achieve the data plane and management plane separation, in conjunction with a firewall. We need to have efficiency of network equipment as well as server equipment.	
Likes 0	
Dislikes 0	
Response	
Ronald Donahey - TECO - Tampa Electric Co. - 1,3,5,6	
Answer	
Document Name	
Comment	
Suggest adding the following from the BCSI section:	

Co-location of BCSI on virtual multi-instance shared environment may be an issue. Are the same requirements applicable there as well?   SIEM tool (no requirement for ESP)

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE

Answer	
Document Name	

Comment

Reflected in our responses is a genuine concern that BES security is not well served by increasing complexity of implementation, operating practices, and compliance obligations. We are not advocating for a lesser security posture but a clear view of the law.

The concern arises from the nature and impact of the proposed revisions and new Standards and Glossary Terms, individually and in total.

If entities cannot understand the obligations, their ability to successfully operate the BES in a responsible, secure, and reliable manner are adversely impacted.

Entities have built their compliance programs and security posture incorporating the existing definitions. To revise programs will cost time and use resources with little associated benefit--redirecting resources from the very security activities on which they need to focus.

We would appreciate if the SDT would assist industry in understanding what security objective is trying to be fulfilled and to better leverage current Standards to minimize complexity, ensure clarity, and promote implementation flexibility.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	
Document Name	

Comment

AEP believes the existing structure of CIP requirements and definitions is sufficient to permit entities to be compliant when using “virtualization” techniques. The proposed definition of Cyber Asset clarifies that the CIP requirements are applicable in a virtual environment.

Likes 0	

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no ISO-NE NYISO NextERA Con-Ed and HQ

Answer

Document Name

Comment

There were no questions on the revision to the BCSI definition.

Is there a difference between the “data about” in the new BCSI definition and the “data in” that is part of the Cyber Asset Definition? Network traffic is neither about or in but in transit. Is network traffic considered BCSI? If not, the change in BCSI definition and the elimination of the EACMS term could cause the monitoring of this traffic to be out of CIP scope.

Likes 0

Dislikes 0

Response

Lauren Price - ATCO Electric - 1 - MRO,RF

Answer

Document Name

Comment

For our industry to maintain security and reliability, we need to break out of the mold of creating new or revised reliability standards that chase cybersecurity. Thought leadership is necessary to position the industry for a more nimble, sustainable, and mature security posture. The industry needs to recognize and accept a paradigm shift to reshape the CIP Standards such that they are written with flexibility and are focused on technology agnostic security objectives to incent Registered Entities to define and implement an adaptive, layered, risk-based cybersecurity program that timely detects, responds to, and mitigates emerging threats. While there has been improvement in the requirement language as the CIP Standards have evolved, they continue to suffer because prescriptive mandatory regulations cannot keep pace with emerging technologies and the rapidly changing cybersecurity threat landscape. Until this paradigm shift occurs, the industry will continue to face the unintended consequences of the current construct, be distracted by the conundrum where security and compliance are at odds, limited in our ability to leverage advances in technology, and will continue to be hindered by the antiquated ideals of a regulation that is chasing cybersecurity.

Likes 0

Dislikes 0

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	
Document Name	

Comment

Reclamation recommends the SDT consider the following:

Principles

The impact rating of a BES Cyber System is determined by its possible impact on the Bulk Electric System, not where it resides (Control Center or any other location) or how it is identified (virtual, non-virtual, hardware, software, etc.), and regardless of a Responsible Entity's functional registration. Following this principle, phrases such as "performing the functional obligations of" are unnecessary.

Instances created within a virtual environment must meet the requirements of the impact rating of that instance.

Hardware used in virtual environments must meet the physical security requirements for the impact rating of the highest rated instance or partition within the hardware.

Recommended Definitions

Reclamation recommends to revise the definition of BES Cyber System as follows:

BES Cyber System – One or more BES Cyber Assets logically grouped to perform one or more reliability tasks. A BES Cyber System may include, but is not limited to:

PCA*

PACS*

EACMS*

Intermediate Systems*

Electronic Access Control Systems: Cyber Assets that control electronic access to BES Cyber Systems.

Virtual Centralized Management System: A centralized system used to administer or configure virtual BES Cyber System(s) or virtual BES Cyber Asset(s).

Virtual Electronic Security Zone: A boundary housing one or more Virtual Machines logically separated from other BES Cyber Systems or other non-BES Cyber Systems using partitioned and isolated service set identifiers (SSIDs), virtual local area networks (VLANs), or other technologies.

Electronic Access Gateway: Cyber Assets (including Electronic Access Points) that control electronic access to and from virtual and non-virtual Electronic Security Perimeter(s).

*Currently defined in the NERC Glossary of Terms.

If the SDT adopts Reclamation's recommended terms and definitions, each term must be added to the NERC Glossary of Terms.

In addition to the recommended terms identified in responses to previous questions, Reclamation also recommends adding the following definition to the NERC Glossary of Terms:

BES Data – Configurations necessary for the operation and security (physical and logical) of the BES.

Rationale

Reclamation recommends virtualization be addressed from the top down, by changing the definition of BES Cyber System.

If each of the new recommended terms is properly described within the recommended revised BES Cyber System definition, the CIP-002 Attachment 1 Impact Rating Criteria will accurately determine the applicable requirements.

Implementation

Reclamation recommends the SDT provide a 24-month implementation plan timeline for entities to comply with the virtualization concepts.

Recommended Impact Rating Criteria

Reclamation recommends simplifying the Impact Rating Criteria using the methodology described below.

BES Cyber Systems are to be rated as high, medium, or low impact as follows:

1. A high impact BES Cyber System has one or more of the following characteristics:
    - Is used to operate transmission lines of 500kV or above
    - Supports a sum greater than 2500kV of transmission lines above 230kV
    - Supports generation with an aggregate capacity greater than 3000MW
    - Is identified as supporting an IROL or is necessary to avoid an Adverse Reliability Impact
2. A medium impact BES Cyber System has one or more of the following characteristics:
    - Supports generation with the aggregate capacity between 1500 – 3000MW
    - Supports a sum between 1500 – 2500kV of transmission lines above 230kV
    - Supports a RAS that could negatively affect an IROL or that can perform automatic Load shedding of 300MW or more
3. A low impact BES Cyber System has one or more of the following characteristics:
    - Supports a sum less than 1500kV of transmission lines above 230kV
    - Supports transmission only between 110 – 230kV
    - Supports generation with an aggregate capacity between 75 – 1500MW
    - Supports any single generator greater than 20MW not already identified as a Medium Impact BES Cyber System
    - Supports any Facilities that are designated a blackstart resource
    - Supports any other RAS not already identified as a medium impact BES Cyber System

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	
Document Name	

Comment

: ERCOT notes that all requirements regarding multi-instance are identified only for BCS. There is not information provided regarding multi-instance used for other asset categories like EACMS and PACS.

Likes 0

Dislikes 0

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE, Group Name Southern Company

Answer

Document Name

Comment

Ensure consistency in the use of terms, such as virtual, hypervisor, host, etc., and be cautious not to use terms that would lock an Entity into a single type of technology.

Likes 0

Dislikes 0

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer

Document Name

Comment

The “instance” and “multi-instance” concept presented throughout the new requirements is not clear. If there is one physical box with multiple virtual Cyber Assets that are a part of the same BES Cyber System, is that considered “multi-instance” and all the new requirements apply or could this be considered one “instance” and be able to protect the entire physical box under the currently approved standards without the additional burdens? For example, an entity has one physical box that houses two virtual High Impact Cyber Assets, a virtual applications server and a virtual database server. Both virtual Cyber Assets are part of one High Impact BES Cyber System. Would the entity be able to protect that physical box as they would today or would they need to also apply the new requirements CIP-005 Part 1.5, Part 1.6, etc.? We believe that the risk associated with the example above is significantly lower compared to a “mixed-mode” environment (CIP/non-CIP or High Impact/EACMS). Additionally, for clarification, if an entity has on physical box that has a High Impact Cyber Asset “instance” and a Medium Impact BES Cyber Asset “instance”, could they continue to protect the physical box at the High Impact level without these additional new requirements?

We fully support the concepts presented, but believe having clearer, approved NERC Glossary of Terms definitions of “instance” and “multi-instance” is necessary. Based on risk, the current CIP requirements provide sufficient protections when virtual CIP systems at the same Impact level reside on one physical box and that physical infrastructure is protected at the same level. Clearly stating that gives the entity the flexibility of no additional burden from

the new requirements, but also allows “mixed-mode” environments. Please consider the following when constructing the definition of *multi-instance:* Virtual systems where the separate instances are a combination of CIP and non-CIP systems or the mixture of BES Cyber System Impact levels.	
Likes 0	
Dislikes 0	
Response	
David Francis - Midcontinent ISO, Inc. - 2,3 - MRO,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	
See comments provided in response to each question under Concept 3. All requirements regarding multi-instance are identified only for BCS. There is not information provided regarding multi-instance used for EACMS.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	
Document Name	
Comment	
Xcel Energy believes that storage virtualization is not adequately addressed above.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	
Document Name	
Comment	

The SPP Standard Review Group agrees with the proposed change in the definition of “Cyber Asset”. However, as we reviewed the document, we noticed that the background information talked about addressing Virtualization, ironically, the proposed language doesn’t discuss or include the term. We would recommend that the drafting team revised the propose language to include the term “Virtualization” and the concepts around it. We feel that this would provide more clarity on what the drafting team’s intents are in reference to the virtualization process.

Additionally, we would suggest adding the management systems to the EACMS Definition instead of breaking them up separately. From our perspective, this provides more stability and reliability when talking about the security of the virtualization process.

Likes 0	
Dislikes 0	

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	
Document Name	

Comment

The definition of Electronic Security Zone is challenging due to the fact that virtualization utilizes shared resources within the hypervisor. There can be shared memory space and shared physical network connections. So virtual machines that are within a shared hypervisor could potentially be sharing resources from non-BES assets. There are very few vendors that can truly create logical separation in a virtualized environment. To mitigate the security risk, any hardware used to host a BES cyber asset virtual machine, should be considered a part of the ESP. Hosting ESP and non-ESP assets on the same hardware introduces the opportunity for code injection into the hypervisor from less stringent environments. With that said, there are vendors that are able to isolate the resources utilized between VM’s of various classifications. One vendor capable of segmentation is Lynx Software Technologies. VMware and Microsoft HyperV are not among the vendors capable of this level of segmentation.

Tacoma Power recommends utilizing industry standards (e.g., NIST) for guidance on mandating policy. Due to the constantly changing nature of virtualization, the slow update process of CIP standards would limit entities from following industry best practices for virtualization security.

Tacoma Power recommends caution in mandating specific security requirements in a virtualized environment. An overarching policy would be far more effective in securing a virtualized environment.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

The existing NERC standards were not developed to consider the technology that currently exists or may be available in the future. In part, this contributes to more constant changes than the NERC standards process can potentially handle. Additionally, in the proposed BCSI definition, it is unclear what the term “pose a security threat” means.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 2 - NPCC	
Answer	
Document Name	
Comment	
There were no questions on the revision to the BCSI definition. Can you provide information about the added value of “processed, organized, structured, or presented in a context” We think that this part could be removed.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	

Document Name	
Comment	
(None)	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	
Document Name	
Comment	
Use of virtualized environments within an ESP is fine, but we disagree with splitting the hypervisor between a control environment (OT) and a business environment. The hypervisor is based on software and it susceptible to zero day exploits and attacks. To be clear, each security zone should have a separate hypervisor (virtualized environment).	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
In consideration of each proposed requirement and definition, entities are asking not only does the idea make sense from a security perspective, but also, what evidence will need to be provided to show compliance with the requirement. The requirements proposed, in many cases, ask for an abstract set of objectives, intent, or principles, all of which may be challenging to demonstrate to an auditor. This should be avoided. Also, any requirement intended for a virtual environment should either be obviously applicable and adaptable to single use physical systems or explicitly exclude those systems from the scope of applicability. None of the proposed requirements consider the possibility of existing systems not being technically capable of meeting the requirement as written. Additionally, the proposed definition of BES Cyber System Information (BCSI) adds the terms “individual security logs,” which is unclear. Does this include single log entries? Further clarification needs to be provided on what is meant by “individual security logs.” The proposed definition of BCSI examples also adds “with network addresses” to network topologies. This implies that network diagrams without network addresses would not be considered BCSI. Is this the SDT’s intent?	
Likes 0	

Dislikes 0

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer

Document Name

Comment

Cowlitz PUD strongly encourages the SDT to continue if efforts in developing standard requirements that support effective implementation of virtual environments with adequate protections.

Likes 0

Dislikes 0

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer

Document Name

Comment

Please address storage in a multi-instance environment.

Likes 0

Dislikes 0

Response

Richard Vine - California ISO - 2

Answer

Document Name

Comment

The ISO supports the comments of the Security Working Group (SWG)

Likes 0

Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	
Document Name	
Comment	
We have proposed the modified EACMS definition to include the management cyber system that can alter the configuration of BCS. Given that the EACMS have been well protected by the current CIP standards, all above requirements regarding CMS may not be necessary if our proposed modification to EACMS is used.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	
Document Name	
Comment	
Suggest adding the following from the BCSI section: Co-location of BCSI on virtual multi-instance shared environment may be an issue. Are the same requirements applicable there as well? SIEM tool (no requirement for ESP)	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
N/A	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	

Comments received from Brandon McCormick – FMPA

1. Do you agree that the proposed change to the Cyber Asset definition makes it inclusive of both physical and virtual devices, including treatment of each virtual machine and hypervisor? If you do not agree, please provide rationale to support your position.

   ☐ Yes
   ☒ No

   Comments: FMPA follows APPA’s comments:

APPA does not agree that the proposed change is inclusive and believes that there is a better way to include both physical and virtual devices. Therefore, public power proposes the following:

> "Programmable electronic devices, including the hardware, software, and data in those devices.
> Virtualized systems or devices are distinct devices."

This proposed change would help in "future-proofing" the definition.

2. Do you agree that the term programmable in the Cyber Asset definition does not need further clarification at this time? If yes, please provide rationale to support your position.

☒ Yes
☐ No
Comments:

3. If programmable does need further clarification, how would you prefer it to be addressed? Use comments to detail necessary definition changes or guidance that could be developed.

Comments:

Centralized Management Systems (CMS)

As the SDT worked through issues related to virtual systems, it became clear that there was no straightforward way within the current CIP Standards to adequately address the risk of systems used to manage virtual environments. Management systems in virtual environments, through their consolidated interfaces and automation, can modify and delete entire infrastructures including virtual servers, networks, and storage. Given the broad capabilities of management systems in a virtual environment, they present specific and significant risk to the reliability of the BES Cyber Systems associated with those management systems.

The SDT considered several options to address the risks of management systems such as grouping management systems into the existing EACMS definition. This, however, would place these assets inappropriately in the EACMS category when they do not perform access control or access monitoring. Using the EACMS category in this manner creates a one-size-fits-all approach to requirements that does not consider the degree of risk or technical constraints posed by the particular system. For example, a system that only monitors and logs access does not pose the same level of risk as a management system for a large virtualized Control Center with the capability to modify or delete a complete infrastructure. Technical controls to mitigate the risk may differ depending on the capabilities of the management system. An electronic access monitoring system presents a risk of leaking BES Cyber System Information; an electronic access control system presents a risk of unauthorized access to, or modification of, a BES Cyber System's operational parameters; and a management system presents a risk of unwanted or unintended modification or deletion of a complete infrastructure. Proposed requirements related to this definition are detailed below.

The SDT determined a more appropriate option was to create a new definition for Centralized Management System (CMS) and apply appropriate and specific security requirements. The SDT seeks comment on the following conceptual definition of Centralized Management System in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

> **Centralized Management System (CMS):**
> A centralized system used for administration or configuration of BES Cyber System(s) through which the configuration of the BES Cyber System can be altered.

4. Do you agree with the proposed definition of Centralized Management Systems (CMS)? If not, please provide rationale to support your position.

☐ Yes
☒ No
Comments:

FMPA agrees with the concept of separating the management plane from the data plane. The definition as proposed should be revised to only include the administration of the BES Cyber System. The current definition may expand the scope to other tools with unintended consequences. Based on group discussions, we have concerns over what is meant by administration or configuration. There were different interpretations based on individual understanding. This should be resolved with a defined term that can be plugged in to the requirements and be implemented by industry.

Virtualization Terms and Requirements

The foundational pieces have now been set for the use of virtualization solutions. However, these solutions still pose risk. These risks and the nature of virtual systems may require some modifications to Standards. The concepts being proposed include additional access control and separation of the management plane from the data plane. This can help to prevent users of the applications on a virtualized system gaining access to the management system that can modify and delete the underlying infrastructure including virtual servers, networks, and storage.

The SDT uses the terms "instance" and "multi-instance" within the proposed requirements below. For the purposes of these proposed changes, the SDT intends for "instance" and "multi-instance" to be understood as:

- Instance: Discrete organizational environments with specific privileges or security levels, consisting of functions that consume resources from the shared infrastructure. Instances are logically isolated but physically interconnected.
- Multi-instance: An environment where a shared infrastructure provides containers for more than one instance.

In reviewing the risks that are unique and inherent to the use of virtualization technologies, the SDT identified the following risks:

1) Shared infrastructure,
2) Span of control, insider threats, and lateral privilege expansion,
3) Misconfiguration, excessive privileges, and capability of administrators, and
4) Escalation of privilege.

The SDT proposes the following definition and requirements in support of the use of virtual technologies.

Electronic Security Zone (ESZ)

The SDT contends that the Electronic Security Perimeter (ESP) definition does not accurately describe the proper isolation of virtual systems within shared infrastructure. Details of the analysis are captured in network isolation portion of the industry webinar presented on March 21, 2017. To address the concerns noted, the SDT seeks comment on the following conceptual definition of Electronic Security Zone (ESZ) in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Electronic Security Zone:
The area defined by the logical separation of one or more Cyber Asset(s).

5. Do you agree that the proposed definition of ESZ more adequately applies to proper isolation of multi-instance environments, regardless of OSI layer? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

FMPA is concerned that there is not enough clarity in the definition of ESZ to separate it from the ESP. ESZs seem to apply in different areas – sometimes they can encompass things like PACS/EACMs that might already fit under different requirements. This confusion of the term will lead to different interpretations and applications of the standard. What does sufficient mean in the “proper isolation of multi-instance environments”?

6. Do you agree that the proposed definition of ESZ would aid the development of future CIP Standards by providing a more relevant level of separation? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

FMPA does not believe that the proposed definition for ESZ would provide the relevant level of separation needed. “Logical separation” is based on current technology and may not be applicable to future controls. VLANs have been a subject of contention in the past with NERC – are these now considered acceptable segregations/boundaries?

New Requirement CIP-005 Requirement 1, Part 1.6

The SDT proposes a new requirement part 1.6 for CIP-005 Requirement R1. This requirement part is for Responsible Entities to implement one or more Electronic Security Zones (ESZ) to meet the security objective of separating the management plane and the data plane of high and medium impact BES Cyber Systems in a multi-instance environment. Part 1.6 would also require Responsible Entities to implement one or more ESZs to meet the security objective of protecting the infrastructure associated with high and medium impact BES Cyber Systems in a multi-instance environment by limiting access to the Centralized Management Systems using a management plane ESZ.

Responsible Entities maintain the flexibility for grouping by cyber system function, by risk, by type of applicable security controls, or other logical groupings. The ESZ contains a distinct subset of the Responsible Entity's Cyber Assets. These are characterized as requiring (or benefiting from) similar security controls and separation from other distinct Cyber Assets. Properly implemented ESZs can limit damage and impact to availability to other surrounding ESZs, specifically by helping protect against span-of-control risks, insider threats, and lateral privilege expansion.

Again, the requirement would only be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS.

Part 1.6:
Logically separate all Applicable Systems into defined groups of one or more Cyber Asset(s) to achieve the objective of mitigating the risks of span-of-control, insider threats, and lateral privilege expansion. At a minimum:
1. The management plane and the data plane of the applicable BES Cyber System shall be separated;
2. The CMS of the applicable BES Cyber System shall be separated from its data plane

7. Do you agree that the proposed CIP-005 Requirement R1, Part 1.6 provides sufficient security controls for the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS to reduce the stated risks inherent to virtualization? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

FMPA is concerned that neither minimum inclusions outlined in Part 1.6 deal with mitigation of span-of-control. In addition, not all vendor solutions may be able to address Part 1.6. The use of the word "achieve" in the draft standard sets a requirement that could be impossible to maintain as new risks emerge. This Requirement should also have the "per device capability" clause.

We recommend changing it as follows:
Logically separate all Applicable Systems, per device capability, into defined groups of one or more Cyber Asset(s) to address potential risks related to span-of-control, insider threats, and lateral privilege expansion.

New Requirement CIP-005 Requirement 1, Part 1.7

Similarly to CIP-005 Requirement R1, Part 1.3, the SDT proposes new requirement Part 1.7. Part 1.7 requires Responsible Entities to identify, control, and explicitly allow only necessary inbound and outbound communication between ESZs of high and medium impact BES Cyber Systems residing in a multi-instance environment. Part 1.7 would be added to CIP-005 to reduce the risks inherent to virtualization related to misconfiguration, excessive privileges, capability of administrators, as well as information protection and data leakage.

The requirement would be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s).

Part 1.7:
Implement technical controls that enforce separation between ESZs by allowing only necessary inbound and outbound communication between the separated Cyber Asset(s) residing in a multi-instance environment.

8. Do you agree that the proposed CIP-005 Requirement R1, Part 1.7 provides a necessary security control to the high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s) to reduce risks inherent to virtualization? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

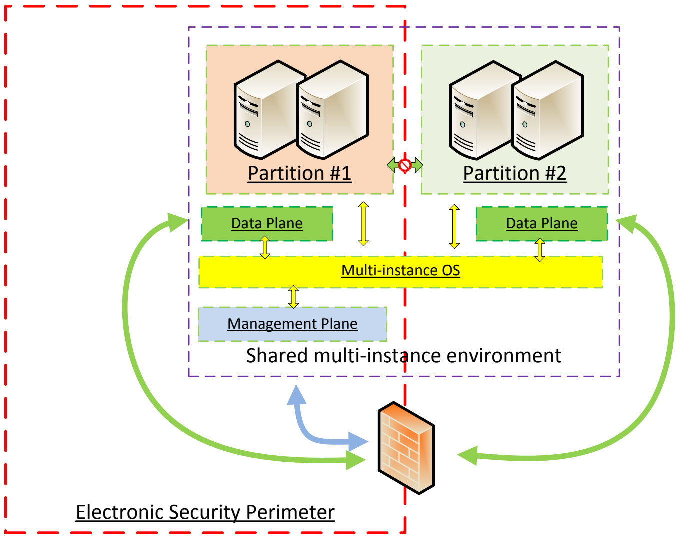
FMPA recommends that the SDT consider the scoping on this requirement part. Would this be identified in the applicability table since it only applies to multi-instance? At the top of the standard/requirement? Or as shown within the requirement? We recommend the SDT provide additional clarity on the ability to have technical controls for other layers (aside from the communication layer) and with shared memory space. We would also like the

SDT to consider the ramifications on the use of a cloud based SIEM vendor who is most likely using a virtualized environment. In the cloud environment, an entity would be transferring risk as well as trust

New Requirement CIP-005 Requirement 1, Part 1.8

Through the SDT work on virtualization, situations have been identified where a Responsible Entity may choose to share the same system infrastructure between applicable Cyber Assets and other programmable devices. As the footprint of cyber assets outside the scope of the CIP Standards in an organization might be significantly larger in size from the Cyber Assets in scope of the CIP Standard, a Responsible Entity may invest in its IT infrastructure with greater capability and more robust features. As presented in the third webinar on virtualization, this is particularly true with storage virtualization implementations. Under certain circumstances, leveraging enterprise infrastructure solutions will provide a better security posture for applicable Cyber Assets. Part 1.8 has been drafted with the objective of allowing such leverage as long as controls mitigating the additional risks are implemented.

A CIP Standard requiring the complete physical separation of applicable Cyber Assets and other programmable devices might adversely affect the overall security posture and reduce operational efficiency for the Responsible Entity through unnecessary expense and complexity of processes or technical implementation. Security controls exist to manage secure logical separation in multi-instance environments and there are operational benefits to sharing a common infrastructure as well. Technological advancements are often coupled with new security mechanisms which often benefit legacy infrastructure.



The diagram above shows an example of a shared multi-instance environment. The green arrows in the diagram represent the data communication. To exchange data between Partition 1 and 2, communication has to go through an EAP represented in the diagram by a firewall. The blue arrows in the diagram represent the management communication. In order to manage Partition 2, or any Cyber Asset hosted by the multi-instance environment and outside the ESP, IP communication to the management plane from outside the ESP has to go through the EAP since the management plan of shared multi-instance environment has to reside inside the ESP. The yellow arrows in the diagram represent the resource management activities performed by the multi-instance operating system necessary to ensure separation of data plane and management plane as well as partitions between Cyber Assets inside the ESP and Cyber Assets outside the ESP.

The SDT proposes CIP-005 Requirement 1, Part 1.8 to provide protection where the infrastructure used in a multi-instance environment is shared between applicable Cyber Assets and other programmable devices. This allows Responsible Entities to leverage the investments and protection of infrastructure shared between applicable Cyber Assets and other programmable devices. The requirement would be applicable to high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS(s).

Part 1.8:

When an infrastructure is shared between BES Cyber Systems and other Cyber Assets not part of a BES Cyber System:

1. The BES Cyber System, the management plane of the shared infrastructure, and any hosted Cyber Assets not part of a BES Cyber Systems shall all be separated; and
2. Communications between the BES Cyber System and any hosted Cyber Assets not part of a BES Cyber System shall all be denied by default

---

9. Do you agree that the proposed CIP-005 Requirement R1, Part 1.8 provides sufficient security control to reduce the risks associated with shared multi-instance environments? If not, please provide a rationale to support your position.

☐ Yes

☒ No

Comments:

There are discrepancies between the language in the Part 1.8 and in the question. Question identifies “shared multi-instance environments “ where the requirement does not. We recommend that the SDT provide guidance on what is infrastructure (possibly using language such as BES related infrastructure) and suggest that the SDT define “Multi-instance”.

If a Jump-host (a required security control for IRA for High BESCS) which is outside of the ESP, then requirement would not be applicable. If the Jump-host was on the VM infrastructure is this a multi-instance environment?

The word “infrastructure” is not defined in the proposed Standard. Consequently, the “infrastructure” on page 4 appears to only include virtual components. APPA questions if this would also include the UPS systems, equipment racks, HVAC systems, floors, lighting, etc.? The “management plane of the shared infrastructure” seems to limit and define “infrastructure” to be components only of the virtual environment.

New Requirement CIP-005 Requirement 3, Part 3.1

In reviewing the risks associated with communications in a virtual environment, the SDT identified a gap with remote access used to perform CMS functions. These communications using a CMS do not align appropriately to Interactive Remote Access. Tasks may be performed from outside the ESP that are a blend of interactive and automated tools, allowing for misinterpretation and unjustified relaxation of security mechanisms required for Interactive Remote Access. Using jump servers to perform CMS functions might not be the most effective or the most secure. Also, remote access to a Cyber Asset inside an ESP could benefit from other methods besides Interactive Remote Access for performing CMS functions.

CIP-005 Requirement R3, Part 3.1 allows for a new type of remote access to be used to perform CMS functions from outside of an ESP. Part 3.1 allows the CMS function to be performed outside an ESP using an access method other than an Intermediate Systems to fix the gap that may exist between

Interactive Remote Access and system-to-system communication. It does this by introducing requirements that are commensurate with the risk inherent to the management function in a multi-instance environment.

The SDT proposes new requirement CIP-005 Requirement 3, Part 3.1. Part 3.1 would be applicable to high and medium impact BES Cyber Systems.

Part 3.1:
Require authentication, integrity and non-repudiation controls for all sessions initiated outside of the ESZ, whether user initiated or system-to-systems communications, used to perform CMS functions.

10. The SDT asserts that the proposed CIP-005 Requirement 1, Part 3.1 provides additional security controls for remote access when performing CMS functions. These are necessary to reduce the risk associated with remote access to multi-instance environments. Do you agree with this assertion? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

FMPA believes that this Requirement conflicts with the implied requirement identified in comments to question 8 that the management plane of the BCS must be inside the ESZ. APPA recommends replacing the proposed language with: "Require authentication, integrity and non-repudiation controls for all CMS functions, per device capability."

If the suggested modification is not used, in the alternative FMPA proposes that this Requirement have the "per device capability" clause.

Encryption of network traffic from CMS to device could make compliance with this Requirement impossible to achieve.

11. Should the gap between Interactive Remote Access and system-to-system communication that was exposed by the examination of the risks inherent to virtualization be addressed for systems other than high and medium impact BES Cyber Systems residing in a multi-instance environment and their associated CMS? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

The NERC standards should be written to address the known risks and not limited to risks associated with managing multi-instance environments.

New Requirement CIP-004 Requirement 4, Part 4.5

The SDT has identified "too much privilege" as an inherent risk in virtualization. This risk can be reduced by adding controls in CIP-004. Limiting of the privileges granted to the minimum necessary is only present in the guidance. It is not a requirement. This security risk can be mitigated, however, by implementation of least privilege access and separation of duties in the requirement language. This means fewer people get high level privileges, and no single individual gets privileges that are too broad. For efficiency, it can be implemented via role-based access control (RBAC), which requires an initial effort to define roles properly. But also provides an opportunity for internal review of the span-of-control risk. Role-based access control and separation of duties are both available in virtual environments. Implementation of RBAC varies by vendor but is generically the same in principle.

The SDT proposes new requirement CIP-004 Requirement 4, Part 4.5. Part 4.5 would be applicable to high and medium impact BES Cyber Systems.

Part 4.5:
The Responsible Entity shall document and implement process(es), except under CIP Exceptional Circumstances, to authorize electronic and unescorted physical access to BES Cyber Systems and BES Cyber Systems Information that implements the principles of need-to-know, least privilege, and separation of duties as determined by the Responsible Entity, as per system capability.

12. The SDT asserts that the new proposed CIP-004 Requirement R4, Part 4.5, provides additional security control to the electronic and unescorted physical access to multi-instance environment processes which reduces the "too much privilege" risk inherent to virtualization which has been identified. Do you agree with this assertion? If not, please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

FMPA recommends that this become Requirement 4 Part 4.2 as the Authorization takes place in 4.1; implementation should become 4.2; then the quarterly review is 4.3, etc. FMPA recommends guidance to small entities that they may identify each role but may need to (resource constrained) add the same person to each role

Concept 2: Modifications to the EACMS definition

As noted above, the SDT reviewed the scope of the current definition, the requirements, and risk of the types of assets contained within EACMS. The current construct does not differentiate controls based on the functionality and risk of the system. The current construct does, however, create what is known as the "hall of mirrors" effect. Specifically, there may be some types of EACMS that should be required to be inside an ESP and behind a firewall. An example could be the management system of a firewall that is categorized in such a way that it must reside within an ESP. That requirement, however, cannot exist for all EACMS because a firewall is itself an EACMS. Without defining a new category, the result would be that every EACMS would need to be inside an ESP and therefore protected by another EACMS. This creates the recursive "hall of mirrors" effect.

There are a number of systems that both monitor and provide part of the solution of controlling access, but do not actually control traffic at the point of entry. These devices or systems may or may not benefit from being inside a protected boundary, or they may form part of the strategy that protects BES Cyber Assets. The technical means of implementing some multi-part systems may require components to be outside, or span the ESP.

To address this, the SDT proposes breaking up the EACMS categorization of applicable systems by function so that the appropriate requirements for each can be applied. The SDT does not, however, want to create a reclassification and documentation exercise for Responsible Entities who would not see benefit and would try to create a way for those Responsible Entities to continue to use EACMS with no changes. There are also other options in addition to these two.

Electronic Access Control System (EACS)

The SDT seeks comment on the following conceptual definition of Electronic Access Control System in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Electronic Access Control System (EACS):

Cyber Assets that perform electronic access control of the BES Cyber Systems. This includes Intermediate Systems.

An Electronic Access Control System performs authentication and authorization of traffic or users. This is the “gatekeeper” function or the classic authentication and authorization functions of standard AAA. In many cases these systems do not perform any active filtering of the traffic passing through any particular interface. The primary duty of EACS is to authenticate and authorize. EACS move beyond the risk of unauthorized access to meta-information about an environment, to unauthorized access to BES Cyber Systems and modification of their operational parameters.

Electronic Access Gateway (EAG)

The SDT seeks comment on the following conceptual definition of Electronic Access Gateway in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Electronic Access Gateway:
Cyber Assets that perform electronic access control of the Electronic Security Perimeter(s). The Electronic Access Gateway also hosts the EAP(s).

An Electronic Access Gateway hosts the EAP and performs the active function of filtering or forwarding traffic at the demarcation point (boundary protection). Primarily, these are firewalls and routers that perform gateway functions at the layer 3 ESP boundary demarcation point.

Electronic Access Monitoring Systems

As technologies and cyber attacks advance and become more complex, Responsible Entities are becoming increasingly interested in collecting and correlating electronic access monitoring events across their enterprises. This broad-based information collection provides Responsible Entities with more visibility into emerging threats and trends. Responsible Entities can then analyze and share this information more readily and take action to improve the overall cybersecurity and reliability of the BES through early detection of compromise.

Under the currently effective CIP Reliability Standards, if a Responsible Entity uses enterprise wide electronic access monitoring tools, the Cyber Assets used to perform the monitoring may meet the definition of EACMS and become subject to the CIP Reliability Standards applicable to EACMS. This may discourage or prevent Responsible Entities from using enterprise wide electronic access monitoring due to the device level requirements of an EACMS. Responsible Entities may be discouraged from providing and correlating security events across enterprise and control networks, even though cyber-attacks against control systems could enter through business networks. The SDT concludes there is value in correlating security events across both control and enterprise networks.

The SDT proposes that the information within the electronic access monitoring systems should be protected as a BCSI repository, rather than having the system categorized as an EACMS. The systems performing electronic access monitoring are used to monitor and collect information about BES Cyber Systems or Electronic Security Perimeter(s) and pose a risk of information leakage. These monitoring systems are not used to control access to the BES Cyber Systems or Electronic Security Perimeter(s). The monitoring function has been in scope of the EACMS definition due to the sensitivity of certain information that may be collected. The proposed change is to treat the data collected through the monitoring capability as BCSI rather than having the monitoring systems categorized as EACMS. This change will enable Responsible Entities to better leverage enterprise-wide monitoring to improve overall situational awareness, and in the process more proactively address security events.

This will result in improved security and reliability. This does not change a Responsible Entity’s obligations to monitor under CIP-007 R4.

To transition electronic access monitoring from EACMS to BCSI, the SDT seeks comment on the following conceptual modification to the definition of BES Cyber System Information in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

Clean:

BES Cyber System Information:

Data about the BES Cyber System that is processed, organized, structured, or presented in a context that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.

BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to gain unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual or collections of IP addresses without context of location and purpose, ESP names, individual security logs, or policy statements.

Examples of BES Cyber System Information may include, but are not limited to: security procedures, collections of security logs, or security configuration information about BES Cyber Systems, Physical Access Control Systems, Electronic Access Control Systems, Electronic Access Gateway Systems, Centralized Management Systems, and Electronic Access Control or Monitoring Systems that are not publicly available; and network topology with network addresses of the BES Cyber System.

Redline:

BES Cyber System Information:

Data ~~Information~~ about the BES Cyber System that is processed, organized, structured, or presented in a context could be used to gain unauthorized access or pose a security threat to the BES Cyber System.

BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual or collections of IP addresses without context of location and purpose, ESP names, individual security logs, or policy statements.

Examples of BES Cyber System Information may include, but are not limited to:~~,~~ security procedures, collections of security logs, or security configuration information about BES Cyber Systems, Physical Access Control Systems, Electronic Access Control Systems, Electronic Access Gateway Systems, Centralized Management Systems, and Electronic Access Control or Monitoring Systems that is not publicly available ~~and could be used to allow unauthorized access or unauthorized distribution~~; ~~collections of network addresses~~; and network topology with network addresses of the BES Cyber System.

Current:

BES Cyber System Information:

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

Proposed Requirements Related to EACMS Changes

Based on the concepts presented above, the table below lists the current requirement scope of EACMS and those proposed for CMS, EACS, and EAG. In the table below, the “X” indicates where the requirement currently applies to the system category in the Applicable Systems column of CIP Standards. The “+” sign indicates an additional requirements being considered to address risk for that specific system category in the Applicable Systems column of CIP Standards. To the extent that there is no difference in requirement applicability, the SDT would look to consolidate the terms into as few classifications as necessary.

Please keep in mind that the SDT does not want to create a reclassification and documentation exercise for Responsible Entities who would not see sufficient benefit and would look to create a way for those Responsible Entities to continue to use EACMS with no changes.

Requirement	EACMS	CMS (+)	EACS (+)	EAG (+)
CIP-004 R1.x		+	+	+
CIP-004 R2.x	X	X	X	X
CIP-004 R3.x	X	X	X	X
CIP-004 R4.x	X	X	X	X
CIP-004 R5.x	X	X	X	X
CIP-005 R1.x		+	+	X (Part 1.5)
CIP-005 R2.x		+		
CIP-005 R3		+		
CIP-007 R1.1	X	X	X	X
CIP-007 R2.x	X	X	X	X
CIP-007 R3.x	X	X	X	X
CIP-007 R4.x	X	X	X	X
CIP-007 R5.x	X	X	X	X
CIP-009 R1.x	X		X	X
CIP-009 R2.1	X		X	X
CIP-009 R2.2	X		X	X
CIP-009 R2.3			+	+
CIP-009 R3.x	X		X	X
CIP-010 R1.x	X	X	X	X

Requirement	EACMS	CMS (+)	EACS (+)	EAG (+)
CIP-010 R2.x	X	X	X	X
CIP-010 R3.1	X	X	X	X
CIP-010 R3.2		X	+	+
CIP-010 R3.3	X	X	X	X
CIP-010 R3.4	X	X	X	X
CIP-010 R3.5	X	X	X	X
CIP-011 R1.x	X	X	X	X
CIP-011 R2.x	X	X	X	X

13. Do you agree with the SDT's assertion that the definition of EACMS is too broad and does not differentiate the capabilities and risk(s) of the systems that fall within that definition scope? If not, please provide rationale to support your position.

☒ Yes
☐ No
Comments:

14. Do you agree that the language of the proposed definitions of EACS provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

☐ Yes
☒ No
Comments: FMPA agrees that the language provides more clarity. However, we are concerned that the change includes intermediate systems, which cannot be inside of the ESP.

15. Do you agree that the language of the proposed definitions of EAG provides better consistency and clarity to the CIP Standards? If not, please provide rationale to support your position and alternative language.

☐ Yes
☒ No
Comments: We agree that the proposed definitions of EAG provides better consistency and clarity; however, the SDT used EAG Systems in the example for the changes to the BCSI definition. Should this be EAG or EAGS?

The SDT used EAG Systems in the example for the changes to the BCSI definition. FMPA is unsure if this should be EAG or EAGS.

16. Do you agree that the current compliance requirements related to EACMS monitoring systems are precluding or discouraging solutions that could reduce risk to security and reliability? Please provide your rationale in support or against this assertion.

☒ Yes
☐ No
Comments:

Yes. The existing standards would make it difficult or potentially impossible to be compliant and use services like Dell Secureworks.

17. Should the security requirements for the access control portion of the EACMS to be different from the monitoring portion of the EACMS? If you do, please provide your rationale.

☒ Yes
☐ No
Comments:

The security controls for monitoring need to be flexible. This is because the BES cannot be negatively impacted solely by a compromise of a monitoring system.

18. Should CIP-011 Requirement R2 scope be expanded to include designated storage locations for access monitoring systems? If not, please provide rationale to support your position.

☐ Yes
☒ No
Comments:

BCSI outside the entities environment should be dealt with in the CIP standards apart from the existing Requirement R2.

19. Do you agree with assignment of CIP Standard requirements to each of the EACS, EAG, and CMS categories as presented in the table above? If not, please provide rationale to support your position.

☒ Yes
☐ No
Comments:

Concept 3: Compliance Guidance

The SDT has explored the idea that no changes are necessary to the CIP Standards to address virtualization. ERO Enterprise-endorsed Compliance Guidance could be used to address many industry concerns with the proper implementation of virtualization.

20. As the standards today do not prohibit the use of virtualization technologies, do you support an approach where no changes are made to the CIP Standards in response to the virtualization issue identified by the V5 TAG? Please provide a rationale to support your position.

☐ Yes
☒ No
Comments:

The current CIP standards do not explicitly prohibit all types of virtualization but require "high water marking" of the impact level even where this is not the most secure and reliable control. For example, the separation of data plane and management plane between hypervisor and guest is a more effective control than applying rigorous CIP Requirements and keeping hypervisors inside the same security zone.

Also, CIP Requirements do not separate the electronic access controls from the electronic access monitoring to allow for different requirements when only monitoring is done. This has a high risk of misallocating scarce resources (money, time, manpower) that could be more effectively applied elsewhere for increased reliability.

Compliance guidance is written to show one or more compliant solutions to clarify and help in applying the Requirements. Such guidance does not supersede standard requirements language. Moreover, such guidance cannot show all possible solutions and is specific and limited, rather than a framework where one can generate new and unique solutions. Solutions currently known to the SDT are only a snapshot in time that may become obsolete at any moment due to technical innovation or changes in the threat environment, while security objectives are more enduring than requirements for a specific solution. Entities may be aware of, or devise a solution unknown to the SDT that provides equal or greater security, that the Requirements language finds the solution non-compliant. Therefore, the proposed standard must emphasize security objectives that allow entities to demonstrate and explain how solutions meets the objective.

Summary

The SDT has provided very diverse concepts for your consideration. Each of these concepts can be moved forward in the drafting process independently. Please provide your responses to each of the questions below.

21. Is your organization in support of Concept 1: Modifications to allow use of secure multi-instance? Please provide rationale to support your position.

☐ Yes
☒ No
Comments:

We would support Concept 1: Modifications to allow use of secure multi-instance provided that comments herein are taken into consideration.

22. Is your organization in support of Concept 2: Modifications to the EACMS definition? Please provide rationale to support your position.

☐ Yes
☒ No
Comments:

We would support Concept 2: Modifications to the EACMS definition provided that comments herein are taken into consideration.

23. Is your organization in support of Concept 3: Compliance Guidance? Please provide rationale to support your position.

☐ Yes
☒ No
Comments:

FMPA believes that the Compliance Guidance would not be appropriate because it only shows limited compliance. Moreover, it does not resolve the issues of high-water marking of impact levels and nor does it allow for the separation of monitoring from EACMS.

24. If you have additional comments that you have not provided in response to the questions above, please provide them here.

Comments:

The existing NERC standards were not developed to consider the technology that currently exists or may be available in the future. In part, this contributes to more constant changes than the NERC standards process can potentially handle.

Additionally, in the proposed BCSI definition, it is unclear what the term “pose a security threat” means.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Unofficial Nomination Form

Project Number 2016-02 Modifications to CIP Standards

Do not use this form for submitting nominations. Use the electronic form to submit nominations by **8 p.m. Eastern, Wednesday, May 23, 2018.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information can be found on the Project 2016-02 Modifications to the CIP Standards page. If you have questions, contact Standards Developer, Jordan Mallory (via email), or at 404-446-2589.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Project 2016-02 Modifications to CIP Standards

This solicitation for nominations is to augment the existing Project 2016-02 Modifications to CIP Standards drafting team that is continuing to address the Standards Authorization Request. NERC is seeking individuals from the United States and Canada who possess experience in one or more of the following areas, but are not limited to:

- Virtualization;
- Cyber Asset and BES Cyber Asset Definitions; and
- Network and Externally Accessible Devices.

Standards Affected

CIP-002-5.1, CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, CIP-011-2, and CIP-012-1.

The time commitment for this project is expected to be up to two face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome.

Name:	
Organization:	
Address:	
Telephone:	
E-mail:	

Please briefly describe your experience and qualifications to serve on the requested Standard Drafting Team (Bio):

If you are currently a member of any NERC drafting team(s), please list each one here:

☐ Not currently on any active SAR or standard drafting team.

☐ Currently a member of the following SAR or standard drafting team(s):

If you previously worked on any NERC drafting team(s), please identify each one here:

☐ No prior NERC SAR or standard drafting team.

☐ Prior experience on the following team(s):

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:

☐ Texas RE
☐ FRCC
☐ MRO
☐ NPCC
☐ RF
☐ SERC
☐ SPP RE
☐ WECC
☐ NA – Not Applicable

Select each Industry Segment that you represent:

☐ 1 — Transmission Owners
☐ 2 — RTOs, ISOs
☐ 3 — Load-serving Entities
☐ 4 — Transmission-dependent Utilities
☐ 5 — Electric Generators
☐ 6 — Electricity Brokers, Aggregators, and Marketers
☐ 7 — Large Electricity End Users
☐ 8 — Small Electricity End Users
☐ 9 — Federal, State, and Provincial Regulatory or other Government Entities
☐ 10 — Regional Reliability Organizations and Regional Entities
☐ NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:

☐ Balancing Authority
☐ Compliance Enforcement Authority
☐ Distribution Provider
☐ Generator Operator
☐ Generator Owner
☐ Interchange Authority
☐ Load-serving Entity
☐ Market Operator
☐ Planning Coordinator
☐ Transmission Operator
☐ Transmission Owner
☐ Transmission Planner
☐ Transmission Service Provider
☐ Purchasing-selling Entity
☐ Reliability Coordinator
☐ Reliability Assurer
☐ Resource Planner

---

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

Provide the names and contact information of two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		E-mail:	
Name:		Telephone:	
Organization:		E-mail:	
Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Nomination Period Open through May 23, 2018

Now Available

Nominations are being sought for additional standard drafting team members through **8 p.m. Eastern, Wednesday, May 23, 2018**.

Use the electronic form to submit a nomination. If you experience difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

The time commitment for this project is expected to be up to two face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome.

Previous drafting or review team experience is beneficial, but not required.

Project 2016-02 Modifications to CIP Standards

This solicitation for nominations is to augment the existing Project 2016-02 Modifications to CIP Standards drafting team that is continuing to address the Standards Authorization Request. NERC is seeking individuals from the United States and Canada who possess experience in one or more of the following areas, but are not limited to:

- Virtualization;
- Cyber Asset and BES Cyber Asset Definitions; and
- Network and Externally Accessible Devices.

Standards Affected

CIP-002-5.1, CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, CIP-011-2, and CIP-012-1.

Next Steps

The Standards Committee is expected to appoint members to the team in June 2018. Nominees will be notified shortly after they have been appointed**.**

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Mat Bunch at (404) 446-9785 or Jordan Mallory at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-7
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.
4. **Applicability:**

    4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. **Balancing Authority**

    4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the requirements in this standard, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirementswhere a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly specified.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between BES Cyber Systems' Logical Isolation Zones.

4.2.3.3. Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-004-7.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program*.

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*.

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.5	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program.*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. EAMS; 3. PACS; 4. PAMS; and 5. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. EAMS; 3. PACS; 4. PAMS; and 5. PCS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations (including EAMS and PAMS whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACS; 2. EAMS; 3. PACS; 4. PAMS; and 5. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. EAMS; 3. PACS; 4. PAMS; and 5. PCS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACS; 2. EAMS; 3. PACS; and 4. PAMS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. EAMS; 3. PACS; and 4. PAMS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACS; 2. EAMS; and 3. PACS; and 4. PAMS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. EAMS; and 3. PACS; and 4. PAMS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, including EAMS and PAMS are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*.

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. EAMS; 3. PACS; 4. PAMS; and 5. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. EAMS; 3. PACS; 4. PAMS; and 5. PCS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACS; 2. EAMS; 3. PACS; 4. PAMS; and 5. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. EAMS; 3. PACS; 4. PAMS; and 5. PCS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACS; 2. EAMS; 3. PACS; and 4. PAMS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. EAMS; and 3. PACS; and 4. PAMS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), including EAMS and PAMS by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.
5.4	High Impact BES Cyber Systems and their associated EACS.	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Systems and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated EACS.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. **Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. **Compliance Monitoring and Assessment Processes:**

   - Compliance Audits
   - Self-Certifications
   - Spot Checking
   - Compliance Violation Investigations
   - Self-Reporting
   - Complaints

   1.4. **Additional Compliance Information:**
   None.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	

The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-7~~6~~
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.
4. **Applicability:**
    - **4.1.** **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.
        - **4.1.1.** **Balancing Authority**
        - **4.1.2.** **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
            - **4.1.2.1.** Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
                - **4.1.2.1.1.** is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
                - **4.1.2.1.2.** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
            - **4.1.2.2.** ~~Each Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
            - **4.1.2.3.** Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner~~Interchange Coordinator or Interchange Authority~~

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the ~~purpose of the~~ requirements in this standard~~contained herein~~, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements~~ in this standard~~ where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly specified~~ explicitly~~.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-7~~6~~:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between- BES Cyber Systems’ Logical Isolation Zones~~discrete Electronic Security Perimeters~~.

4.2.3.3. Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

~~4.2.3.2.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.3.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.4.~~4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-004-7~~6~~.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R1 – Security Awareness Program*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7~~6~~ Table R1 – Security Awareness Program

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program*.

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.2	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access ~~to applicable Cyber Assets~~, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program*.

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~and~~ 2. PACS; and ~~2.~~3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S;~~ and~~ 2. PACS; and ~~2.~~3. PCS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~and~~ 2. PACS; and ~~2.~~3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; ~~and~~ 2. PACS; and ~~2.~~3. PCS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.3	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~and~~ 2. PACS; and ~~2.~~3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; ~~and~~ 2. PACS; and ~~2.~~3. PCS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~and~~ 2. PACS; and ~~2.~~3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; ~~and~~ 2. PACS; and ~~2.~~3. PCS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.5	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~and~~ 2. PACS; and ~~2.~~3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; ~~and~~ 2. PACS; and ~~2.~~3. PCS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R4 – Access Management Program.*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~and~~ ~~1.~~2. EAMS; 3. PACS; 4. PAMS; and ~~2.~~5. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; ~~and~~ ~~1.~~2. EAMS; 3. PACS; 4. PAMS; and ~~2.~~5. PCS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations (including EAMS and PAMS)~~,~~ whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

CIP-004-7~~6~~ Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.2	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~and~~ ~~1.~~2. EAMS; 3. PACS; 4. PAMS; and ~~2.~~5. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; ~~and~~ ~~1.~~2. EAMS; 3. PACS; 4. PAMS; and ~~2.~~5. PCS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~1.~~2. EAMS; ~~and~~ 3. PACS; and ~~2.~~4. PAMS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; ~~1.~~2. EAMS; ~~and~~ 3. PACS; and ~~2.~~4. PAMS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-7~~6~~ Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.4	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~1.~~2. EAMS; and 3. PACS; and ~~2.~~4. PAMS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; ~~1.~~2. EAMS; and 3. PACS; and ~~2.~~4. PAMS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, including EAMS and PAMS are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R5 – Access Revocation*.

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~and~~ ~~1.~~2. EAMS; 3. PACS; 4. PAMS; and ~~2.~~5. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; ~~and~~ ~~1.~~2. EAMS; 3. PACS; 4. PAMS; and ~~2.~~5. PCS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7~~6~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.2	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~and~~ ~~1.~~2. EAMS; 3. PACS; 4. PAMS; and ~~2.~~5. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; ~~and~~ ~~1.~~2. EAMS; 3. PACS; 4. PAMS; and ~~2.~~5. PCS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7~~6~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.3	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; ~~1.~~2. EAMS; ~~and~~ 3. PACS; and ~~2.~~4. PAMS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; ~~1.~~2. EAMS; and 3. PACS; and ~~2.~~4. PAMS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), including EAMS and PAMS by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.
5.4	High Impact BES Cyber Systems and their associated~~:~~ EAC~~M~~S.	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber ~~Assets~~ Systems and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated ~~:~~ EAC~~M~~S.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. **Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. **Compliance Monitoring and Assessment Processes:**

   - Compliance Audits
   - Self-Certifications
   - Spot Checking
   - Compliance Violation Investigations
   - Self-Reporting
   - Complaints

   1.4. **Additional Compliance Information:**
   None.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	

The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

1. **Title:** Cyber Security —BES Cyber System Logical Isolation

2. **Number:** CIP-005-7

3. **Purpose:** To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication.

4. **Applicability:**

   4.1. Functional Entities: For the requirements in this standard, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are explicitly specified.

      4.1.1. Balancing Authority

      4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

            4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the requirements in this standard, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly specified.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between BES Cyber Systems' Logical Isolation Zones.

4.2.3.3. Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Date:

See Implementation Plan for CIP-005-7.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes to mitigate the risk posed by unauthorized communications to and from applicable systems that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Logical Isolation Zones.* These processes exclude consideration of time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Logical Isolation Zones* and additional Evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R1 – Logical Isolation Zones			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Have one or more methods to logically isolate applicable systems, either individually or as a group, by only allowing: 1.1.1. Communication that has documented inbound and outbound access permissions, including the reason for granting access; and 1.2.1. Serial port connectivity such as RS-232 and RS-485. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Evidence may include, but is not limited to, configuration of systems that enforce logical isolation such as network infrastructure configuration (ACL, VLAN, VXLAN, MPLS), compute configuration (e.g., Hypervisor, containers), storage system configuration (e.g., SAN, NAS, DAS).

CIP-005-6 Table R1 – Logical Isolation Zones			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems and their associated PCS	Protect the data traversing communication networks used to provide connectivity between components of a Logically Isolated Zone that spans multiple geographic locations to preserve confidentiality and integrity.	Evidence may include, but is not limited to, architecture documents detailing the methods used to mitigate the risk of unauthorized disclosure. Examples include physical protection and the points where encryption initiates and terminates.
1.3	High Impact BES Cyber Systems with Dial-up Connectivity and their associated PCS Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated PCS	Perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.4	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems at Control Centers and their associated PCS	Have one or more methods for detecting known or suspected malicious inbound and outbound communications to and from applicable systems either individually or as grouped in Part 1.1, excluding serial port connectivity such as RS-232 and RS-485.	Evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, privileged introspection, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes to mitigate the risk posed by exploitation of Interactive Remote Access that collectively include the applicable requirement parts, per system capability, in *CIP-005-6 Table R2 –Remote Access Management*.

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7 Table R2 Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems and their associated PCS	Have one or more methods to ensure that Interactive Remote Access to applicable systems is through an Intermediate System that is isolated from the BES Cyber System and restricts Interactive Remote Access to only authorized users.	Evidence may include, but is not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems and their associated PCS	Have one or more methods to mitigate the risks posed by unauthorized modification and unauthorized disclosure of data during all Interactive Remote Access sessions that terminate at an Intermediate System.	Evidence may include, but is not limited to, architecture documents detailing the methods used to mitigate the risk of unauthorized disclosure. Examples include illustrating where encryption initiates and terminates.

CIP-005-7 Table R2 Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associate PCS Medium Impact BES Cyber Systems and their associated PCS	Have one or more methods to require multi-factor authentication for all Interactive Remote Access sessions.	Evidence may include, but is not limited to, documents detailing the authentication factors used.

CIP-005-7 Table R2 Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems and their associated PCS	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Evidence may include, but is not limited to documented methods such as: • Methods for accessing logged information or monitoring to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as requiring vendors to call and request a second factor to initiate remote access.

CIP-005-7 Table R2 Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems and their associated PCS	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Evidence may include, but is not limited to, documented methods, such as: • Methods to disable vendor remote access for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes to mitigate the risk posed by unrestricted access for communication between the management plane [1] and the data plane[2] that collectively include the applicable requirement parts, in *CIP-005-6 Table R3* – Isolation of Management Plane and Data Plane.

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R3* – Isolation of Management Plane and Data Plane and additional evidence to demonstrate implementation as described in the Measures column of the table.

---

[1] Management plane of a system is that element that configures, monitors, and provides management, monitoring and configuration services to, all layers of the network stack and other parts of the system.

[2] Data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic.

CIP-005-6 Table R3 – Isolation of Management Plane and Data Plane			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACS 2. PCS Medium Impact BES Cyber Systems and their associated PCS: 1. EACS 2. PCS	Have one or more methods per system capability to: 1. Restrict access to the management plane; and 2. Logically isolate the management plane from the data plane.	An example of evidence may include but is not limited to documentation that includes the following: Configuration of systems that enforce authentication and logical isolation such as network infrastructure configuration (ACL, VLAN, VXLAN, MPLS), compute configuration (e.g. Hypervisor, containers), storage system configuration (e.g. SAN, NAS, DAS).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	

The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

1. **Title:** Cyber Security —~~-~~BES Cyber System Logical Isolation~~Electronic Security Perimeter(s)~~

2. **Number:** CIP-005-7~~6~~

3. **Purpose:** To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication.~~manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.~~

4. **Applicability:**

   4.1. Functional Entities: For the ~~purpose of the~~ requirements in this standard~~contained herein~~, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are explicitly specified.~~ explicitly.~~

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

~~**4.1.6.**~~**4.1.5. Reliability Coordinator**

~~**4.1.7.**~~**4.1.6. Transmission Operator**

~~**4.1.8.**~~**4.1.7. Transmission Owner**

4.2. Facilities: For the ~~purpose of the~~ requirements in this standard~~contained herein~~, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly specified.~~ explicitly.~~

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-7~~6~~:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between BES Cyber Systems' Logical Isolation Zones~~discrete Electronic Security Perimeters~~.

~~**4.2.3.2.**~~**4.2.3.3.** Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.5.**~~**4.2.3.6.** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Date:

See Implementation Plan for ~~Project 2016-03~~CIP-005-7.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes to mitigate the risk posed by unauthorized communications to and from applicable systems ~~-~~that collectively include each of the applicable requirement parts in *CIP-005-7~~6~~ Table R1 – Logical Isolation Zones.* These processes exclude consideration of time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE) ~~*Electronic Security Perimeter*~~.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7~~6~~ Table R1 – Logical Isolation Zones* ~~*-Electronic Security Perimeter*~~ and additional Evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation Zones

Part	Applicable Systems	Requirements	Measures
1.1~~3~~	~~Electronic Access Points for~~ High Impact BES Cyber Systems ~~Electronic Access Points for~~ Medium Impact BES Cyber Systems	Have one or more methods to logically isolate applicable systems, either individually or as a group, by only allowing: 1.1.1. ~~Require~~Communication that has documented inbound and outbound access permissions, including the reason for granting access; and~~, and deny all other access by default.~~ 1.2.1. Serial port connectivity such as RS-232 and RS-485. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Evidence may include, but is not limited to, configuration of systems that enforce logical isolation such as network infrastructure configuration (ACL, VLAN, VXLAN, MPLS), compute configuration (e.g., Hypervisor, containers), storage system configuration (e.g., SAN, NAS, DAS). ~~An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.~~

CIP-005-6 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation Zones			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems and their associated PCS	Protect the data traversing communication networks used to provide connectivity between components of a Logically Isolated Zone that spans multiple geographic locations to preserve confidentiality and integrity.	Evidence may include, but is not limited to, architecture documents detailing the methods used to mitigate the risk of unauthorized disclosure. Examples include physical protection and the points where encryption initiates and terminates.
1.3~~4~~	High Impact BES Cyber Systems with Dial-up Connectivity and their associated PCS ~~A~~ Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated PCS~~A~~	~~Where technically feasible, P~~perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets~~.~~ per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.4~~5~~	~~Electronic Access Points for~~ High Impact BES Cyber Systems and their associated PCS ~~Electronic Access Points for~~ Medium Impact BES Cyber Systems at Control Centers and their associated PCS	Have one or more methods for detecting known or suspected malicious inbound and outbound communications to and from applicable systems either individually or as grouped in Part 1.1, excluding serial port connectivity such as RS-232 and RS-485.	~~An example of e~~Evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, privileged introspection, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes to mitigate the risk posed by exploitation of Interactive Remote Access that collectively include the applicable requirement parts, ~~where technically feasible,~~per system capability, in *CIP-005-6 Table R2 –Remote Access Management*.

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-7~~6~~ Table R2 ~~– Remote Access Management~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated ~~:~~ PCS~~A~~ Medium Impact BES Cyber Systems ~~with External Routable Connectivity~~ and their associated ~~:~~ PCS~~A~~	Have one or more methods to ~~For all Interactive~~ ensure that Interactive Remote Access~~,~~ to applicable systems is through an Intermediate System that is isolated from the BES Cyber System and restricts Interactive Remote Access to only authorized users. ~~utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~	E~~xamples of e~~vidence may include, but ~~are~~ is not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated ~~:~~ PCS~~A~~ Medium Impact BES Cyber Systems ~~with External Routable Connectivity~~ and their associated~~:~~	Have one or more methods to mitigate the risks posed by unauthorized modification and unauthorized disclosure of data during ~~For~~ all Interactive Remote Access sessions~~,~~ that terminate at an Intermediate System ~~utilize~~	~~An example of e~~Evidence may include, but is not limited to, architecture documents detailing the methods used to mitigate the risk of unauthor~~e~~ized disclosure. Examples include illustrating where encryption initiates and terminates.

CIP-005-7~~6~~ Table R2 ~~– Remote Access Management~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~•~~ PCS~~A~~	~~encryption that terminates at an Intermediate System~~.	
2.3	High Impact BES Cyber Systems and their associate ~~d:~~ PCS ~~A~~ Medium Impact BES Cyber Systems ~~with External Routable Connectivity~~ and their associated PCS~~A~~	Have one or more methods to ~~R~~require multi-factor authentication for all Interactive Remote Access sessions.	~~An example of e~~Evidence may include, but is not limited to, ~~architecture~~ documents detailing the authentication factors used. ~~Examples of authenticators may include, but are not limited to,~~ ~~Something the individual knows such as passwords or PINs. This does not include User ID;~~ ~~Something the individual has such as tokens, digital certificates, or smart cards; or~~ ~~Something the individual is such as fingerprints, iris scans, or other biometric characteristics.~~

Formatted: Space Before: 0 pt, After: 0 pt, Add space between paragraphs of the same style, Line spacing: single, No bullets or numbering, Don't keep with next

CIP-005-7~~6~~ Table R2 ~~– Remote Access Management~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their ~~associated~~associated ~~:~~ PCS ~~A~~ Medium Impact BES Cyber Systems ~~with External Routable Connectivity~~ and their associated ~~:~~ PCS~~A~~	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	~~Examples of e~~Evidence may include, but is~~are~~ not limited to documented methods such as: • Methods for accessing logged information or monitoring ~~information~~ to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as requiring vendors to call and request ~~calling and requesting~~ a second factor to~~in order to~~ initiate remote access.

CIP-005-7~~6~~ Table R2 ~~– Remote Access Management~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated ~~•~~ PCS~~A~~ Medium Impact BES Cyber Systems ~~with External Routable Connectivity~~ and their associated ~~•~~ PCS~~A~~	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	~~Examples of e~~Evidence may include, but ~~are~~ is not limited to, documented~~ion of the~~ methods~~(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access)~~, such as: • Methods to disable vendor remote access ~~at the applicable Electronic Access Point~~ for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

Formatted: Add space between paragraphs of the same style, Line spacing: single, No bullets or numbering

Formatted: Space Before: 0 pt, Add space between paragraphs of the same style, Line spacing: single, No bullets or numbering

R3. Each Responsible Entity shall implement one or more documented processes to mitigate the risk posed by unrestricted access for communication between the management plane[1] and the data plane[2] that collectively include the applicable requirement parts, in *CIP-005-6 Table R3* – Isolation of Management Plane and Data Plane.

---

[1] Management plane of a system is that element that configures, monitors, and provides management, monitoring and configuration services to, all layers of the network stack and other parts of the system.

[2] Data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic.

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R3* – Isolation of Management Plane and Data Plane and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R3 – Isolation of Management Plane and Data Plane			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACS 2. PCS Medium Impact BES Cyber Systems and their associated PCS: 1. EACS 2. PCS	Have one or more methods per system capability to: 1. Restrict access to the management plane; and 2. Logically isolate the management plane from the data plane.	An example of evidence may include but is not limited to documentation that includes the following: Configuration of systems that enforce authentication and logical isolation such as network infrastructure configuration (ACL, VLAN, VXLAN, MPLS), compute configuration (e.g. Hypervisor, containers), storage system configuration (e.g. SAN, NAS, DAS).

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	

The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the requirements in this standard, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are explicitly specified.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the requirements in this standard, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly specified.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-7:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between BES Cyber Systems' Logical Isolation Zones. .

4.2.3.3 Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-006-7.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan*.

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; and 2. PCS	Use at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS	Where technically feasible, use two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; and 2. PCS	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; and 2. PCS	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: - High Impact BES Cyber Systems, or - Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; and 2. PCS	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; and 2. PCS	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.10	High Impact BES Cyber Systems and their associated PCS Medium Impact BES Cyber Systems at Control Centers and their associated PCS	Restrict physical access to cabling and other nonprogrammable communication components used for applicable systems in the same Logical Isolation Zone in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program.*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; and 2. PCS	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the escorted access process was implemented, such as visitor logs.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; and 2. PCS	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the escorted access process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; and 2. PCS	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program*.

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months, Also, additional evidence such as dated maintenance records or other documentation to demonstrate that testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

D. **None**Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to

Version	Date	Action	Change Tracking
			use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	

The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7~~6~~

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the ~~purpose of the~~ requirements in this standard~~contained herein~~, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements~~ in this standard~~ where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are explicitly specified~~ explicitly~~.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~4.1.6~~4.1.5 **Reliability Coordinator**

~~4.1.7~~4.1.6 **Transmission Operator**

~~4.1.8~~4.1.7 **Transmission Owner**

4.2. **Facilities:** For the ~~purpose of the~~ requirements in this standard~~contained herein~~, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements ~~in this standard~~ where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly specified~~ explicitly~~.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard ~~CIP-006-6~~CIP-006-7:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Assets associated with communication networks and data communication links between~~-~~ BES Cyber Systems' Logical Isolation Zones. ~~discrete Electronic Security Perimeters~~.

4.2.3.3 Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

~~**4.2.3.2**~~**4.2.3.4** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.3**~~**4.2.3.5** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.4**~~**4.2.3.6** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates:

See Implementation Plan for CIP-006-7~~6~~.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7~~6~~ Table R1 – Physical Security Plan*.

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7~~6~~ Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7~~6~~ Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-7~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~	Use~~tilize~~ at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.3	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~	Where technically feasible, use~~tilize~~ two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-7~~6~~ Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.5	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-7~~6~~ Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-7~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.8	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-7~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.9	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

~~CIP-006-6~~CIP-006-7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.10	High Impact BES Cyber Systems and their associated PCS~~A~~ Medium Impact BES Cyber Systems at Control Centers and their associated ~~:~~ PCS~~A~~	Restrict physical access to cabling and other nonprogrammable communication components used for ~~connection between~~ applicable ~~Cyber Assets~~systems ~~within~~ in the same ~~Electronic Security~~Logical Isolation Zone ~~Perimeter~~ in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: • encryption of data that transits such cabling and components; or • monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or • an equally effective logical protection.	An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, -one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R2 – Visitor Control Program.*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7~~6~~ Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter~~,~~ ~~except during CIP Exceptional Circumstances~~.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the escorted access process was implemented, such as visitor logs.

CIP-006-7~~6~~ Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.2	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor~~, except during CIP Exceptional Circumstances~~.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the escorted access process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R3 – Maintenance and Testing Program*.

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7~~6~~ Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months, Also, ~~and~~ additional evidence such as dated maintenance records or other documentation ~~to demonstrate that this testing was done, such as dated maintenance records, or other documentation~~ to demonstrate that ~~showing~~ testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of	

Version	Date	Action	Change Tracking
		Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	

The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

1. **Title:** Cyber Security — System Security Management
2. **Number:** CIP-007-7
3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**
   - **4.1. Functional Entities:** For the requirements in this standard, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are explicitly specified.
     - **4.1.1. Balancing Authority**
     - **4.1.2. Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
       - **4.1.2.1.** Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
         - **4.1.2.1.1.** is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
         - **4.1.2.1.2.** performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
       - **4.1.2.2.** Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
       - **4.1.2.3.** Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the requirements in this standard, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly specified.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-007-7:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between BES Cyber Systems' Logical Isolation Zones (LIZ).

4.2.3.3. Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. Effective Dates: See Implementation Plan for CIP-007-7.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by uncontrolled logical and physical connectivity that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – Connectivity*.

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – Connectivity* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1– Connectivity			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Use one or a combination of the following methods (per system capability) excluding serial port connectivity such as RS-232 and RS-485: • Configure each system to provide only essential logical connectivity; • Detect and alert on malicious communication within systems; • Baseline system logical connectivity, and alert on deviation from baseline; or • Other method(s) to mitigate the risk posed by uncontrolled logical connectivity. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled logical ports. • Listings of logical listening ports on the applicable systems, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others. • Documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, privileged introspection, etc.) are implemented within systems. • Any necessary combination of configuration files of system connectivity, storage connectivity, or network connectivity.

CIP-007-7 Table R1– Connectivity			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. PCS; and 2. Nonprogrammable communication components located inside both a PSP and a LIZ. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCS; and 2. Nonprogrammable communication components located inside both a PSP and a LIZ.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by unmanaged software that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Software Management*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Software Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Software Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Use one or a combination of the following methods (per system capability) to allow only essential software execution, as determined by the Responsible Entity: • Configure each system with intentionally installed essential software and executable scripts; • Baseline currently installed software and executable scripts and alert on any newly installed software or executable scripts; • Implement application whitelisting; • Use read-only bootable media; or • Other methods to mitigate the risk posed by unmanaged software. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to: • Documentation of essential software and executable scripts; • Application whitelisting rule sets; • Documentation of read-only bootable media configuration; or • Documentation of other methods.

R3. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by malicious code that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention*.

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Deploy method(s) to deter, detect, or prevent malicious code. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Mitigate the threat of detected malicious code. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to monitor security events to mitigate the risk posed by detectable security incidents that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*.

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Log events (per system capability) for identification and subsequent investigations of Cyber Security Incidents that include each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types that the BES Cyber System can detect and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Generate alerts for security events that the Responsible Entity determines need an alert, that include, as a minimum, each of the following types of events (per system capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to, paper or system-generated lists of security events that the Responsible Entity determined need alerts, including paper or system generated lists showing how alerts are configured.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACS; 2. PACS; and 3. PCS	Retain applicable event logs identified in Part 4.1 per system capability for at least the last 90 consecutive calendar days.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by unauthorized electronic access that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*.

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
5.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Have a method(s) to enforce authentication of interactive user access, per system capability. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location or by system type(s). NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.
5.3	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are put in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the system; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the system.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

		NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACS; 2. PACS; and 3. PCS	Per system capability, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: - System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or - Attestations that include a reference to the documented procedures that were followed.
5.7	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACS; 2. PACS; and 3. PCS	Per system capability, either: - Limit the number of unsuccessful authentication attempts; or - Generate alerts after a threshold of unsuccessful authentication attempts. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: - Documentation of the account-lockout parameters; or Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:
- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	

The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7~~6~~

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the ~~purpose of the~~ requirements in this standard~~contained herein~~, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are explicitly specified.~~ explicitly.~~

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the~~ SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner~~Interchange Coordinator or Interchange Authority~~

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the ~~purpose of the~~ requirements in this standard~~contained herein~~, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly specified.~~ explicitly.~~

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-007-7~~6~~:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between BES Cyber Systems’ Logical Isolation Zones (LIZ).~~discrete Electronic Security Perimeters.~~

4.2.3.3. Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. **Effective Dates:** See Implementation Plan for CIP-007-7~~6~~.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by uncontrolled logical and physical connectivity that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R1 – ~~Ports and Services~~Connectivity*.

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R1 – ~~Ports and Services~~Connectivity* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~Connectivity			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems ~~with External Routable Connectivity~~ and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	~~Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.~~ Use one or a combination of the following methods (per system capability) excluding serial port connectivity such as RS-232 and RS-485: - Configure each system to provide only essential logical connectivity; - Detect and alert on malicious communication within systems; ~~or~~ - Baseline system logical connectivity, and alert on deviation from baseline; or - Other method(s) to mitigate the risk posed by uncontrolled logical connectivity. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: - Documentation of the need for ~~all enabled ports on~~ all enabled logical ports. ~~applicable Cyber Assets and Electronic Access Points, individually or by group.~~ - Listings of logical ~~the~~ listening ports on the ~~Cyber Assets~~ applicable systems, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or - Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others. - Documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, privileged introspection, etc.) are implemented within systems. - Any necessary combination of configuration files of system connectivity, storage connectivity, or network connectivity.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~Connectivity

Part	Applicable Systems	Requirements	Measures
1.2	High Impact BES Cyber Systems and their associated: 1. PCS~~A~~; and 2. Nonprogrammable communication components located inside both a PSP and a~~n~~ ~~ESP~~LIZ. Medium Impact BES Cyber Systems at Control Centers and their associated: 1. PCS~~A~~; and 2. Nonprogrammable communication components located inside both a PSP and a~~n~~ ~~ESP~~LIZ.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by unmanaged software that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R2 – ~~Security Patch~~ Software Management*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R2 – ~~Security Patch~~Software Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R2 – ~~Security Patch~~Software Management			
Part	Applicable Systems	Requirements	Measures

2.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	~~A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.~~ Use one or a combination of the following methods (per system capability) to allow only essential software execution, as determined by the Responsible Entity: • Configure each system with intentionally installed essential software and executable scripts; • Baseline currently installed software and executable scripts and alert on any newly installed software or executable scripts; • Implement application whitelisting; ~~or~~ • Use read-only bootable media; or • Other methods to mitigate the risk posed by unmanaged software. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to:~~, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.~~ • Documentation of essential software and executable scripts; • Application whitelisting rule sets; • Documentation of read-only bootable media configuration; or • Documentation of other methods.

R3. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by malicious code that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R3 – Malicious Code Prevention*.

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R3 – Malicious Code Prevention

Part	Applicable Systems	Requirements	Measures
3.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	Deploy method(s) to deter, detect, or prevent malicious code. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-7~~6~~ Table R3 – Malicious Code Prevention

Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	Mitigate the threat of detected malicious code. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: - Records of response processes for malicious code detection - Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to monitor security events to mitigate the risk posed by detectable security incidents that collectively include each of the applicable requirement parts in *CIP-007-6 Table R4 – Security Event Monitoring*.

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	Log events ~~at the BES Cyber System level~~ (per ~~BES Cyber S~~system capability~~) or at the Cyber Asset level (per Cyber Asset capability~~) for identification ~~of,~~ and ~~after-the-fact~~ subsequent investigations of~~,~~ Cyber Security Incidents that include~~s, as a minimum,~~ each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types that the ~~for which the~~ BES Cyber System ~~is capable of~~can detect~~ing -~~and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	Generate alerts for security events that the Responsible Entity determines need ~~necessitates~~ an alert, that include~~s~~, as a minimum, each of the following types of events (per ~~Cyber Asset or BES Cyber S~~system capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to, paper or system-generated lists~~ing~~ of security events that the Responsible Entity determined need~~cessitate~~ alerts, including paper or system generated lists showing how alerts are configured.

CIP-007-6 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCSA~~A~~ Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCSA~~A~~	~~Per system capability~~ ~~Where technically feasible, r~~Retain applicable event logs identified in Part 4.1 per system capability for at least the last 90 consecutive calendar days. ~~except under CIP Exceptional Circumstances.~~	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PCSA~~A~~	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, ~~any~~ findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by unauthorized electronic access that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R5 – System Access Controls*.

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
5.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	Have a method(s) to enforce authentication of interactive user access, ~~where technically feasible.~~ per system capability. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location~~,~~ or by system type(s). NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.
5.3	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-6 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	Change known default passwords, per ~~Cyber Asset~~system capability	Examples of evidence may include, but are not limited to: - Records of a procedure that passwords are changed when new devices are put in production; or - Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the ~~Cyber Asset~~system; and 5.5.2. ~~5.5.2~~ Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the ~~Cyber Asset~~system.	Examples of evidence may include, but are not limited to: - System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or - Attestations that include a reference to the documented procedures that were followed.

		NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	

CIP-007-7~~6~~ Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.6	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	~~Where technically feasible~~Per system capability, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: - System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or - Attestations that include a reference to the documented procedures that were followed.
5.7	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	~~Where technically feasible~~Per system capability, either: - Limit the number of unsuccessful authentication attempts; or - Generate alerts after a threshold of unsuccessful authentication attempts. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	Examples of evidence may include, but are not limited to: Documentation of the account-lockout parameters; or - Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

- The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:
- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information:

None.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	

The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Management

2. **Number:** CIP-010-4

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability management requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the requirements in this standard, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are explicitly specified.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the requirements in this standard, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements where a specific type of Facilities, systems, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly specified.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-4:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between BES Cyber Systems' Logical Isolation Zones (LIZ)..

4.2.3.3. Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Date:

See Implementation Plan for CIP-010-4.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by insecure system configuration that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Secure Configuration Management*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R1 – Secure Configuration Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R1 – Secure Configuration Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Control change to the Secure Configuration implemented on systems through: 1.1.1. Authorization; 1.1.2. Prior to the change, determine required cyber security controls in the Secure Configuration that could be impacted by the change; 1.1.3. Implementation; and 1.1.4. Following the change, verify that required cyber security controls determined in 1.1.2 are not adversely affected and document the results. The process requirements of Parts 1.1.1 through 1.1.4 and timeline are based on the analysis of the risk to BES reliability and the risk posed by the change to the system(s).	Examples of evidence may include, but are not limited to: • Records of authorization • Records of controls impact evaluation; • Records of implementation; and • Records of verification.

1.2	High Impact BES Cyber Systems	For each change that deviates from the implemented Secure Configuration, perform the following, per system capability, except during CIP Exceptional Circumstances: 1.2.1. Prior to implementing any change in the production environment, test the changes in a test environment; or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the Secure Configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of tested cyber security controls, test dates, successful test results, and a list of differences between the production and test environments including descriptions of how any differences in the test and production environments were accounted for.

CIP-010-4 Table R1 – Secure Configuration Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.3: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing Secure Configuration associated with installing or updating operating system, firmware, and software and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the Secure Configuration change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by unauthorized change to Secure Configurations that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Secure Configuration Monitoring.*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R2 – Secure Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4Table R2 – Secure Configuration			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS	Use one or a combination of the following methods to monitor the implemented Secure Configuration (per system capability): • Hash monitoring; • Configuration monitoring; • Configuration auditing; or • Other method(s) to mitigate the risk posed by unauthorized change to Secure Configurations. The process requirements of Part 2.1 and timeline are based on the analysis of the risk to BES reliability and the impact rating of the applicable system(s).	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.
2.2	High Impact BES Cyber Systems and their associated: 1. EACS; and 2. PCS	Investigate and remediate detected unauthorized changes to the implemented Secure Configuration found through implementation of Requirement R2 Part 2.1.	An example of evidence may include, but is not limited to, records of unauthorized change investigations and remediating activities.

CIP-010-4Table R2 – Secure Configuration			
Part	**Applicable Systems**	**Requirements**	**Measures**
		The process requirements of Part 2.2 and timeline are based on the analysis of the risks to BES reliability and the risks posed by the detected unauthorized change to the implemented Secure Configuration	

R3. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by system vulnerabilities that collectively include each of the applicable requirement parts in *CIP-010-4 Table R3– Vulnerability Management*.

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4 Table R3 – Vulnerability Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4 Table R3 – Vulnerability Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-4 Table R3 – Vulnerability Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Per system capability, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the Secure Configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4 Table R3 – Vulnerability Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PCS	Prior to adding a new Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements and additions of the same type of Cyber Asset with a Secure Configuration that models an existing Secure Configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the addition) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

CIP-010-4 Table R3 – Vulnerability Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Identify software vulnerabilities using one or more of the following methods: • Vulnerability database monitoring; • Patch source monitoring; • Vulnerability scanning; or • Other method(s) to identify software vulnerabilities. The process of Part 3.5 shall include the periodicity for identifying software vulnerabilities based on the risk to BES reliability and the impact rating of the applicable system(s).	An example of evidence may include, but is not limited to: • Records of vulnerability database monitoring; • Records of patch source monitoring; or • Records of vulnerability scanning.

CIP-010-4 Table R3 – Vulnerability Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.6	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Create or update a plan to mitigate the identified software vulnerabilities from Part 3.5, through one or more of the following: • Implementing security patches; • Applying compensating controls; • System hardening; or • Other method(s) to mitigate software vulnerabilities. The plan for Part 3.6 must include the timeline for mitigating the software vulnerability based on the analysis of the risk posed by the software vulnerability to the applicable systems. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to: • Records of implemented security patches; • Records of applied compensating controls; • Records of system hardening; or • Records of other methods.

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Systems, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1 Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber System, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber System; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber System.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

The Background, VRF/VSLs, and Guidelines and Technical Basis Sections have been removed for this informal posting. The Project 2016-02 is seeking comments around the concept of the Requirement/Measure language at this time. All other sections will be modified prior to the initial posting.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability ~~Assessments~~ Management

2. **Number:** CIP-010-4~~3~~

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability ~~assessment~~ management requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the ~~purpose of the~~ requirements in this standard~~contained herein~~, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements ~~in this standard~~ where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are explicitly specified.~~ explicitly.~~

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

~~**4.1.4.**~~ **Generator Owner**

~~**4.1.5.**~~**4.1.4.** ~~**Interchange Coordinator or Interchange Authority**~~

~~**4.1.6.**~~**4.1.5. Reliability Coordinator**

~~**4.1.7.**~~**4.1.6. Transmission Operator**

~~**4.1.8.**~~**4.1.7. Transmission Owner**

4.2. Facilities: For ~~the purpose of~~ the requirements ~~contained herein~~in this standard, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements ~~in this standard~~ where a specific type of Facilities, systems, or equipment or subset of Facilities, systems, and equipment are applicable, these are explicitly specified. ~~explicitly.~~

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-4~~3~~:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between~~-~~ BES Cyber Systems' Logical Isolation Zones (LIZ).~~discrete Electronic Security Perimeters~~.

~~4.2.3.2.~~4.2.3.3. Cyber Assets associated with communication networks and data communication links used to extend a Logical Isolation Zone to more than one geographic location.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Date:

See Implementation Plan for ~~Project 2016-03~~CIP-010-4.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by insecure system configuration that collectively include each of the applicable requirement parts in *CIP-010-4~~3~~ Table R1 – Secure Configuration ~~Change~~ Management*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~ 4 Table R1 – Secure Configuration ~~Change~~ Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4~~3~~ Table R1 – Secure Configuration ~~Change~~ Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~1.1~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Develop a baseline configuration, individually or by group, which shall include the following items:~~ ~~1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;~~ ~~1.1.2. Any commercially available or open-source application software (including version) intentionally installed;~~ ~~1.1.3. Any custom software installed;~~ ~~1.1.4. Any logical network accessible ports; and~~ ~~1.1.5. Any security patches applied.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• Documentation A spreadsheet identifying the required items of the baseline secure configuration for each Cyber Assetsystem, individually or by group.; or~~ ~~A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.~~

1.1~~2~~	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	Control change to the S~~s~~ecure C~~c~~onfiguration ~~described in CIP-010 Requirement R1 Part 1.1~~ implemented on systems through: ~~Authorize and document changes that deviate from the existing baseline configuration.~~ ~~1.1.1.~~ 1.1.1. Authorization; 1.1.2. Prior to the change, determine required cyber security controls in the Secure Configuration that could be impacted by the change; 1.1.3. Implementation; and 1.1.4. Following the change, verify that required cyber security ~~controls determined~~controls determined in 1.1.2 are not adversely affected~~;~~ and document the results. ~~.~~ The process requirements of Parts 1.1.1 through 1.1.4 and timeline are based on the analysis of the risk to BES reliability and the risk posed by the change to the system(s).	Examples of evidence may include, but are not limited to: • ~~A change request record and~~ R~~r~~ecords ~~for~~of authorization~~associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or~~ • Records of ~~testing~~controls impact ~~evaluaton~~evaluation; • Records of implementation; and • Records of ~~evaluation~~verification. ~~Documentation that the change was performed in accordance with the requirement.~~

CIP-010-4~~3~~ Table R1 – Secure Configuration ~~Change~~ Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~1.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~EACMS;~~ ~~PACS; and~~ ~~PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~EACMS;~~ ~~PACS; and~~ ~~PCA~~	~~For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.~~	~~An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.~~
~~1.4~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For a change that deviates from the existing baseline configuration:~~ ~~Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;~~ ~~Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and~~ ~~Document the results of the verification.~~	~~An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.~~

1.2~~5~~	High Impact BES Cyber Systems	~~Where technically feasible, f~~For each change that deviates from the ~~existing baseline~~ implemented Secure C~~c~~onfiguration, perform the following, per system capability, except during CIP Exceptional Circumstances: 1.2.1. Prior to implementing any change in the production environment, test the changes in a test environment; or ~~-~~test the changes ~~test the changes~~ in a production environment where the test is performed in a manner that minimizes adverse effects, that models the ~~baseline~~ Secure C~~c~~onfiguration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.2.~~2~~2.~~3~~ Document the results of the testing and,~~. and, i~~if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation	An example of evidence may include, but is not limited to, a list of tested cyber security controls, test dates, ~~tested along with~~ successful test results, and ~~and~~ a list of differences between the production and test environments including ~~with~~ descriptions of how any differences in the test and production environments were ~~addressed.~~accounted for ~~how any differences were accounted for~~.~~,~~ ~~including of the date of the test.~~

CIP-010-4~~3~~ Table R1 – Secure Configuration ~~Change~~ Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		between the test and production environments.	
1.3~~6~~	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.3~~6~~: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to a change that deviates from the existing ~~baseline~~ Secure C~~c~~onfiguration associated with installing or updating ~~baseline CIP-007-7 R2 and CIP-010-4 R3 Part 3~~operating system, firmware, and software~~.6secure configuration items in Parts 1.1.1, 1.1.2, and 1.1.5,~~ and when the method to do so is available to the Responsible Entity from the software source: 1.3~~6~~.1. Verify the identity of the software source; and 1.3~~6~~.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the ~~baseline~~ Secure Configuration change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by unauthorized change to Secure Configurations that collectively include each of the applicable requirement parts in *CIP-010-4~~3~~ Table R2 – Secure Configuration Monitoring.*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4~~3~~ Table R2 – Secure Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~3~~ 4Table R2 – Secure Configuration ~~Monitoring~~

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; and 2. PCS~~A~~	Use one or a combination of the following methods to monitor the implemented Secure Configuration (per system capability): ~~Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.~~ • Hash monitoring; • Configuration monitoring; • Configuration auditing; or • Other method(s) to mitigate the risk posed by unauthorized change to Secure Configurations. The process requirements of Part 2.1 and timeline are based on the analysis of the risk to BES reliability and the impact rating of the applicable system(s).	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.
2.2	High Impact BES Cyber Systems and their associated:	Investigate and remediate detected unauthorized changes to the	An example of evidence may include, but is not limited to, records of

CIP-010-~~3~~ 4Table R2 – Secure Configuration ~~Monitoring~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACS; and 2. PCS	implemented Secure Configuration found through implementation of Requirement R2 Part 2.1. The process requirements of Part 2.2 and timeline are based on the analysis of the risks to BES reliability and the risks posed by the detected unauthorized change to the implemented Secure Configuration	unauthorized change investigations and remediating activities.

R3. Each Responsible Entity shall implement one or more documented process(es) to mitigate the risk posed by system vulnerabilities that collectively include each of the applicable requirement parts in *CIP-010-~~3~~4 Table R3– Vulnerability ~~Assessments~~Management*.

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-4~~3~~ Table R3 – Vulnerability ~~Assessments~~ Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-4~~3~~ Table R3 – Vulnerability ~~Assessments~~Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~4~~3 Table R3 – Vulnerability ~~Assessments~~Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	~~Where technically feasible,~~ Per system capability, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the ~~baseline~~ Secure C~~c~~onfiguration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-4~~3~~ Table R3 – Vulnerability ~~Assessments~~Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PCS~~A~~	Prior to adding a new ~~applicable~~ Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances~~,~~ and like replacements and additions of the same type of Cyber Asset with a ~~baseline~~ Secure C~~c~~onfiguration that models an existing ~~baseline~~ Secure C~~c~~onfiguration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the~~-~~ addition~~new Cyber Asset~~) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~ Medium Impact BES Cyber Systems and their associated: 1. EAC~~M~~S; 2. PACS; and 3. PCS~~A~~	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

CIP-010-~~4~~3 Table R3 – Vulnerability ~~Assessments~~Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Identify software vulnerabilities using one or more of the following methods: • Vulnerability database monitoring; • Patch source monitoring; • Vulnerability scanning; or • Other method(s) to identify software vulnerabilities. The process of Part 3.5 shall include the periodicity for identifying software vulnerabilities based on the risk to BES reliability and the impact rating of the applicable system(s).	An example of evidence may include, but is not limited to: • Records of vulnerability database monitoring; • Records of patch source monitoring; or • Records of vulnerability scanning.

CIP-010-~~4~~3 Table R3 – Vulnerability ~~Assessments~~Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.6	High Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS Medium Impact BES Cyber Systems and their associated: 1. EACS; 2. PACS; and 3. PCS	Create or update a plan to mitigate the identified software vulnerabilities from Part 3.5, through one or more of the following: • Implementing security patches; • Applying compensating controls; • System hardening; or • Other method(s) to mitigate software vulnerabilities. The plan for Part 3.6 must include the timeline for mitigating the software vulnerability based on the analysis of the risk posed by the software vulnerability to the applicable systems. NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.	An example of evidence may include, but is not limited to: • Records of implemented security patches; • Records of applied compensating controls; • Records of system hardening; or • Records of other methods.

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber ~~Assets~~Systems, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	

CIP-010-4~~3~~ - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1 Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber ~~Assets~~System, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber ~~Assets~~System; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber ~~Assets~~System.

CIP-010-4~~3~~ - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards
October 29, 2018, Informal Posting

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Cyber Asset (CA)	Programmable electronic devices, including the hardware, software, and data in those devices.	A p~~P~~rogrammable electronic device~~s~~, including the physical or virtual hardware, software, and data in th~~os~~e device~~s~~.
BES Cyber System (BCS)	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	Any combination of hardware (including virtual hardware), software (including application virtualization), and data, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse	Retired

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber ~~Asset~~ System (PCS~~A~~) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber ~~Asset~~System (BCS), • ~~network within an~~ A BES Cyber System Logical Isolation Zone ~~Electronic Security Perimeter (ESP)~~ containing high or medium impact BES Cyber Systems, or • PCS~~A~~ associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.	Cyber systems ~~Assets~~ that control~~, alert, or log~~ access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Access Monitoring Systems (PAMS)	N/A	Cyber systems that alert or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	Retired
Protected Cyber System (PCS)	N/A	Cyber systems that are able to communicate with a BES Cyber System from within the BES Cyber System's Logical Isolation Zone. The impact rating of Protected Cyber Systems is equal to the highest rated BES Cyber System within the Logical Isolation Zone.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	Retired
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	RETIRED – Proposed Develop EAMS and EACS
Electronic Access Control System (EACS)	N/A	Cyber systems that provide electronic access control to BES Cyber Systems.
Electronic Access Monitoring Systems (EAMS)	N/A	Cyber systems that provide electronic access monitoring of BES Cyber Systems.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	Retired
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Logical Isolation Zone via a bi-directional routable protocol connection.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Logical Isolation Zone (LIZ)	N/A	A logical security zone created by applying controls to communications to or from BES Cyber Systems and Protected Cyber Systems.
Intermediate Systems (IS)	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	A system acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access to authorized users.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated access by a person employing a remote access client to a BES Cyber System or Protected Cyber System from outside of a Logical Isolation Zone. Interactive Remote Access does not include system-to-system process communications or access initiated from an Intermediate System.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which~~,~~ ~~BES Cyber Assets,~~ BES Cyber Systems~~,~~ or Electronic Access Control ~~or Monitoring~~ Systems reside~~,~~ and for which access is controlled.
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber ~~Asset~~System, ~~a network within an ESP,~~ or a Protected Cyber ~~Asset~~System. ~~Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~
Secure Configuration	N/A	The implemented set of controls supporting the security objectives found within the CIP Reliability Standards where the following text exists within the requirement language: “NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.”

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards | Virtualization

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System to submit comments on the **Virtualization Updates for CIP-004, CIP-005, CIP-006, CIP-007, CIP-010, and Associated Definitions**. Comments must be submitted by **8 p.m. Eastern, Tuesday, December 18, 2018**

Additional information is available on the project page. If you have questions, contact Standards Developer Jordan Mallory (via email) or at (404) 446-2589.

Background Information

Project 2016-02 (1) addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and (2) considers the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for Standard Drafting Team Consideration (V5TAG Transfer Document).

The V5TAG, which consisted of representatives from NERC, Regional Entities and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP Version 5 standards and to support industry's implementation activities. During the V5TAG's activities, it identified certain issues with the CIP Reliability Standards that would be better addressed by a standard drafting team (SDT) for the CIP Reliability Standards. The V5TAG developed the CIP Version 5 Transition Advisory Group Issues for Consideration document to formally recommend that the SDT address these issues and consider modifications to the standard language during the standards development process. Among other issues, the V5TAG stated "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

As the SDT investigated these issues, it found that virtualization affects most of the technical definitions used within CIP from the foundational "Cyber Asset" to the technical CIP standards (CIP-005, CIP-007, and CIP-010 in particular). This is due to virtualization changing fundamental assumptions, such as the standards having an "electronic device" basis and focusing on routable protocol level only, perimeter-based security. The SDT found virtualization to be not only a driver of change, but a symptom of a larger issue with the standard's ability to adapt to current and future technology innovation. The SDT concluded these more technical standards could benefit from removing inherent prescription of certain architectures and moving requirements to an objective or results-oriented level that do not make assumptions about architecture. In other words, the standards should not go further and prescribe how to secure today's newer architectures but should require that certain security objectives be met and "get out of the way" of virtualization and future innovations that can increase reliability, resiliency, and security of our BES Cyber Systems.

The SDT has been addressing these issues and is at a point where enough work has been accomplished to post the SDT's work in progress and get industry feedback on the direction. The SDT has progressed from a general direction of "cyber system orientation and objective-level requirements" to now having many of these concepts drafted into these standards. During this informal comment period, the SDT recognizes that this is a work in progress and is not ready for a formal posting and ballot and is seeking industry feedback on the direction and concepts of these definitions and requirements.

The remaining CIP standards are not directly affected by virtualization or technology changes and the SDT believes only conforming changes will be required in those standards. As part of our Standard Authorization Request, the SDT also addressed the addition of CIP Exceptional Circumstances allowances where needed. Therefore, the SDT is also posting CIP-004 and CIP-006 for three reasons:

- to show what the conforming changes from the SDT's virtualization work may look like;
- to begin to show how the EACMS split into EACS and EAMS would affect these standards;
- to show the new CIP Exceptional Circumstances additions within these standards.

Summary of Definition Changes

The following provides rationale and updates the associated definitions.

Term to be retired	Rationale for Retirement
BES Cyber Asset	This term is proposed for retirement and the foundational definition is established at the system level.
Electronic Access Control or Monitoring Systems	Term is proposed for retirement and split into two new proposed terms; Electronic Access Control Systems (EACS); and Electronic Access Monitoring Systems (EAMS).
Protected Cyber Asset	This term is proposed for retirement and the concepts of the term are incorporated into the proposed definition of Protected Cyber System (PCS). This change takes advantage of the more objective-based requirements at the system level.
Electronic Access Point	With the proposed retirement of CIP-005-6 Part 1.2 this definition is no longer required. The isolation concepts in proposed requirement Part 1.1 address the necessary controls previously defined in the concept of an identified Electronic Access Point.
Electronic Security Perimeter	This term is proposed for retirement. The concepts of the ESP have been incorporated into the definition of a Logical Isolation Zone (LIZ)

The CIP SDT Proposed new or revised definitions to incorporate virtualization and future technology. The bullet points below provide rationale for a number of the definitions. Please see the CIP Definitions document for all new and revised definitions.

- **Cyber Asset –** The SDT is proposing to retain the Cyber Asset definition with updates to incorporate virtual hardware. With the proposed updates, it is only used in places where it did not make sense to upgrade the term to cyber system. Cyber Asset can be located in the TCA and Removable Media definitions and in a small number of locations in the CIP-010 standard. The goal is to limit the use of 'Cyber Asset' to areas where the upgraded term 'Cyber System does not apply.
- **BES Cyber System –** This term was updated to accommodate the cyber system concept. The hardware portions of the new definition were incorporated from the Cyber Asset definition and qualifying language (15 mins, etc.) included from the BES Cyber Asset definition. The term no longer relies on the word "programmable" and uses new language to classify devices.
- **EACMS to EACS and EAMS –** To support wider correlation of events and data sharing with government agencies and other security vendors to more quickly detect cyber-attacks, the SDT is proposing to split off cyber systems that do electronic access monitoring but perform no electronic access control. The new terms, EACS and EAMS will allow changes within the applicability for the monitoring portion to allow third party monitoring systems. This allows adjustments to the applicability of requirements that are appropriate to the different risks associated with EACS and EAMS.
- **Physical Access Control System (PACS) –** During the process of evaluating the split in applicability for EACMS the SDT determined that the PACS definition would need the same considerations to ensure consistency for monitoring systems. The alerting and logging definition parts were removed from the definition and moved to a new proposed term, Physical Access Monitoring Systems (PAMS). The SDT is seeking input from industry on whether or not having PACS and PAMS as two separate definitions is a positive path for the future.
- **Logical Isolation Zone (LIZ) –** The SDT is proposing this new term which transitions to a new zone-based protection model to control communications to and from BES Cyber Systems and Protected Cyber Systems taking advantage of advances in cyber security. The SDT intends for this concept to be backwards compatible with the ESP while also being non-prescriptive to the communications protocol and layer of the Open Systems Interconnection (OSI) model in which they are implemented.
- **Physical Security Perimeter (PSP) –** In concert with the changes to EACMS and PACS, the SDT is proposing the removal of the requirement for monitoring systems to be kept inside of a PSP. This change would allow flexibility for security monitoring services to be outsourced where these types of controls are currently not available.

Summary of CIP-005 Changes

For a detailed explanation of these changes, please refer to the *CIP-005 Technical Rationale* document.

- **ESP transition to Logical Isolation Zone –** To accommodate advances in network security that go beyond routable protocol address filtering at perimeters, the SDT is proposing a transition to the zone concept while retaining backward compatibility with ESPs.

- **Super ESP, 4.2.3.2 and 4.2.3.3 Exemptions, and R1.2 –** As it addresses virtualization, the SDT is concurrently addressing the V5TAG issue known as the "Super ESP," where BES Cyber Systems may be split across different geographic locations within a single ESP.
- **Management Plane isolation –** Virtualization allows BES cyber systems with a 15 minute impact to share infrastructure with systems that do not share that time constraint (e.g., a control system and its historian). The SDT has added a new requirement (R3) to bring the management plane and its isolation controls into scope of the CIP standards.

Summary of CIP-007 Changes

For a detailed explanation of these changes, please refer to the *CIP-007 Technical Rationale* document.

- Made conforming changes to applicable systems column: (PCS, EACS, etc.)
- Made conforming changes to ensure the requirements are at the system level (per system capability, remove references to Cyber Asset, etc.)
- Added security objectives to the "Big R" main requirements. Example: Each Responsible Entity shall implement one or more documented process(es) *to mitigate the risk posed by uncontrolled logical and physical connectivity* that collectively include each of the applicable requirement parts in…"
- Modified R1.1 (ports/services) to be more objective oriented. Permits use of east/west IDS, baselining logical connectivity, etc. in addition to documenting required network accessible ports.
- Introduced new requirement for installing only essential software and executable scripts on high and medium impact BES Cyber Systems, EACS, PACS, and PCAs.
- Moved CIP-007 R2 patching requirement to CIP-010 vulnerability management program requirement
- Added CIP Exceptional Circumstances language to apply to all of Requirement 4 (Security Event Monitoring)

Summary of CIP-010 Changes

For a detailed explanation of these changes, please refer to the *CIP-010 Technical Rationale* document.

- Made conforming changes to applicable systems column (PCS, EACS, etc.)
- Made conforming changes to ensure the requirements are at the system level (per system capability, remove references to Cyber Asset, etc.)
- Added security objectives to the "Big R" main requirements. Example: Each Responsible Entity shall implement one or more documented process(es) *to mitigate the risk posed by insecure system configuration* that collectively include each of the applicable requirement parts in…"
- Removed the requirement to develop a baseline configuration
- Introduced the concept of a secure configuration. This new concept requires the collective identification of the methods used to comply with the security requirements in CIP-005 R1, CIP-007 R1, R2, R3, R4, R5, and CIP-010 R3.
- Replaced prescriptive timeframes with a risk based evaluation for entity determined timeframes.

- Added specification to the configuration monitoring requirement for hash monitoring, configuration monitoring, or configuration auditing.
- Split obligation to investigate detected unauthorized changes to its own requirement part. Added obligation to remediate detected unauthorized changes.
- Moved patch management requirement from CIP-007 to the CIP-010 Vulnerability Management program. Rephrased requirement in terms of identifying and mitigating software vulnerabilities. Added risk-based entity defined timeframes for implementation.
- Added CIP Exceptional Circumstances to apply to testing of changes prior to implementation

Questions

1. The proposed BCS definition no longer relies on the term Cyber Asset. The SDT asserts that the proposed BES Cyber System definition describes the BCS adequately without the use of the word "programmable" in the definition. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

2. The SDT asserts that the proposed Cyber Asset definition provides clarity around virtual hardware. (Cyber Assets revised definition: Programmable electronic devices, including the physical or virtual hardware, software, and data in those devices.) Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

3. The SDT asserts that the term Cyber Asset should continue to be used within the NERC Glossary of Terms for: Removable Media and Transient Cyber Asset. Due to the nature of that type of hardware, these devices do not lend themselves to the systems approach. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

4. The SDT is proposing to retire EACMS and develop two new terms: EACS and EAMS. These terms will allow changes within the applicability for the monitoring portion to allow third party monitoring systems. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

☐ Yes

☐ No

Comments:

5. The SDT realized through the process of splitting EACMS that the same considerations apply to PACS, which will allow changes within the applicability for alerting and logging (PAMS is not reflected within the applicability section at this time). The SDT is considering splitting the PACS term into PACS and PAMS to allow third party monitoring or event correlation to be performed without carrying the PACS classification. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

6. The SDT is proposing to move away from the more prescriptive ESP/EAP model to logical isolation through the higher level objectives provided by the BES Cyber System concept and its Logical Isolation Zone. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

7. The SDT is considering taking qualitative language out of the Intermediate System definition and using it to clarify requirements. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

8. The SDT is considering changes to the ERC and IRA definitions to address V5TAG issues (see the CIP-005 Technical Rationale document for detailed information). ERC will have conforming changes only and will continue its use as a scoping mechanism. The proposed modifications to IRA will apply to certain non-routable to routable protocol conversion scenarios. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

   ☐ Yes

   ☐ No

   Comments:

9. To the extent possible, the SDT intends its modifications to permit approaches to compliance that are “backwards compatible” with compliance approaches within the currently approved versions of the CIP standards. (Notable exceptions include CIP-005 R3, CIP-007 R2, and Secure Configurations –

CIP-010). Do you agree the modifications are backwards compatible? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

☐ Yes

☐ No

Comments:

10. The SDT has not yet determined a proposed timeframe to include in the Implementation Plan. How long would you as an entity need to implement the proposed modifications? Please provide your implementation timeframe and justification for why that amount of time would be needed.

Comments:

11. The SDT is proposing conforming modifications to CIP-004. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

    a. Modifications related to CIP Exceptional Circumstances

    b. Use of newly proposed terms EACS and EAMS in the Applicable Systems column

    c. Addition of PCS to the Applicable System column for Parts in CIP-004 to mitigate security risks associated with individuals not needing authorization or PRAs when granted access to systems inside the Logical Isolation Zone

☐ Yes

☐ No

Comments:

12. The SDT is proposing modifications to CIP-005 (see the CIP-005 Technical Rationale document for detailed information). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

    a. The replacement of the ESP concept with Logical Isolation Zone (LIZ).

    b. Is the backward compatibility clear as existing ESPs and EAPs move to the new LIZ concept?

    c. The addition of the 4.2.3.3 exemption in the standard along with the addition of Requirement part R1.2 to address the V5TAG concern of “Super ESPs” or single networks within or between BES Cyber Systems that span more than one geographic location.

    d. As differing forms of shared infrastructure come into play with virtualization, Requirement R3 has been added to include the management plane and its isolation controls as a part of the CIP standards. Is this concept clearly and widely understood?

☐ Yes

☐ No

Comments:

13. The SDT is proposing conforming modifications to CIP-006. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:
    a. Modifications related to CIP Exceptional Circumstances
    b. Use of newly proposed term EACS in the Applicable Systems column

    ☐ Yes

    ☐ No

    Comments:

14. The SDT is proposing modifications to CIP-007 (see the CIP-007 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:
    a. The SDT is proposing adding the security objectives throughout the Requirements in CIP-007. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?
    b. The SDT is proposing the security objective in CIP-007 R1, "to mitigate the risk posed by uncontrolled logical and physical connectivity". Do you agree that the modifications to CIP-007 R1 Part 1.1 fulfill this security objective for systems where connectivity is not limited to TCP/IP port service combinations, as in virtualized systems and SAN based storage?
    c. Do you agree that the modifications to CIP-007 R1 Part 1.1 add necessary flexibility to fulfill the security objective of CIP-007 R1 for virtualized systems and provides a degree of future proofing?

    ☐ Yes

    ☐ No

    Comments:

15. The SDT is proposing modifications to CIP-010 (see the CIP-010 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:
    a. The SDT is proposing adding the security objectives throughout the Requirements in CIP-010. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?
    b. The SDT is proposing to modify the referenced baseline configuration from CIP-010-3 R1 Part 1.1 to a 'Secure Configuration' which is made up of the implemented controls that fulfill requirements within CIP-005 and CIP-007. Do you agree that this set of controls supports managing change under CIP-010 R1 Part 1.1?
    c. The SDT is proposing to modify the current CIP-007 R2 requirements and move them to CIP-010 R3. The SDT believes that the software vulnerability management found within this set of requirements fits logically within the security objective of CIP-010 R3 "to mitigate the risk posed by system vulnerabilities" and has moved it there. Do you agree?

d. The SDT is proposing CIP-010 R3 Parts 3.5 and 3.6 to replace the current CIP-007 R2 Parts 2.1 – 2.4. Do you agree that the proposed CIP-010 R3 Parts 3.5 and 3.6 offer the additional flexibility needed when implementing virtualized systems that can be dormant for a period, and for which security patches have become available?

☐ Yes

☐ No

Comments:

16. Provide any additional comments for the SDT to consider, if desired.

Comments:

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Technical Rationale and Justification for Reliability Standard CIP-005-7

November 2018

DRAFT – WORK IN PROGRESS

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. The Standard Drafting Team (SDT) is proposing changes to CIP-005-6 as it updates the standards based on technology innovation and changes such as the increasing use of virtualization.

CIP-005 - From ESP's to "Logical Isolation" – The Case for Change

In previous versions of the CIP standards, CIP-005 required declarations of Electronic Security Perimeters (ESP) based on OSI layer 3 routable protocols. All BES Cyber Assets (BCA) that were connected to a network with routable protocols had to reside inside a declared ESP. Any External Routable Connectivity (ERC) to the BES Cyber Assets inside the ESP had to enter and exit via an Electronic Access Point (EAP). This limited the traffic entering or leaving the ESP to only that which was needed. It denied all other traffic by default.

This "castle and moat with drawbridge" protection, where the castle is the BES Cyber Systems (BCS), the moat is the ESP, and the drawbridge is the EAP, has been in place for many years. For a number of situations, it still offers sufficient protection. This protection configuration, however, drives certain network architecture decisions that may hinder the adoption of newer and in some cases more secure designs. Network access control is expanding beyond perimeter-based security at routable protocol address levels into other levels, with security present within the network fabric itself. The entire network is becoming "the firewall." As infrastructure components become smarter, entities can describe network policy at layers other than that of a routable protocol address, and the infrastructure itself can enforce these access policies at multiple levels.

The nature of virtualization is driving much of this as workloads are dynamically created, moved, and destroyed to meet changing demand. With virtualization, what resides in an ESP might be very dynamic, and rulesets in any EAPs will need to be dynamic as well. This is driving solutions more towards policy-based user access controls for workloads that the infrastructure then dynamically applies within the environment. EAPs themselves are also dynamic, and as network access controls become embedded into the infrastructure, we may go from a few designated EAPs to thousands of dynamic locations where access controls are enforced.

This is the reason the CIP standards are changing from "perimeters" to "zones" and why the ESP has been replaced with the Logical Isolation Zone (LIZ). A perimeter typically implies an outer boundary; something you can draw a rectangle around on a network diagram. As network security becomes more integrated into the network fabric, or is virtualized and dynamic, it is no longer a perimeter that you can draw a box around. This is driving us to employ the zone construct for the future. An ESP is one form of logical isolation zone making it backward compatible, but a logical isolation zone can be broader than the layer 3, routable protocol subnet.

As firewalls continue to evolve, IP addresses and port numbers, which are simply protocol data, will become less common methods of identifying and filtering communications. What needs to be secured are the processes behind those layer 3 network addresses and the actual communications they are processing. IP addresses and ports have traditionally been filtered at the network layer to ensure communications include only what is needed. As technology continues to evolve, more secure future architectures may not be based on routable protocol addressing schemes.

Logical Isolation – What Does It Mean?

ESPs deal only with layer 3 routable protocol addressing. Virtualization and its accompanying shared infrastructure has other characteristics such as shared computing hosts, shared storage, shared virtual networks and switches, all of which posing new security concerns. To adapt to these changes, CIP-005 includes a requirement that high and medium impact BES Cyber Systems be “logically isolated” from all other systems (regardless of protocol) to replace the routable protocol-based ESP requirement.

If a BCS is executing on a virtual host along with another related virtual machine that may not have a 15-minute impact, (e.g. a control system and its data historian), the entity must either consider all these workloads as part of a single system or declare the system with the 15-minute impact as a BCS and the historian as a separate system. If the latter is chosen, the entity will need to prove that the two systems are logically isolated and that every communication between the two is limited to only what is necessary.

Logical isolation is also relevant to other layers of a computing stack. Imagine in a virtualized data center where you are looking at a BES Cyber System architecture “from the side”. You can see the different layers of the system, from the storage on a Storage Area Network (SAN) through the virtual networks, switches, and firewalls at the virtual network layer, up to the virtual hosts that are executing the application workloads. If you rotate the view until you are looking down at the system from above, you should be able to see the touch points of all these layers to other systems. Logical isolation refers to this top-down view. An entity needs to be able to show that only necessary data flows are allowed through any of these layers that have an interface to another system. For example, at a storage layer, BCS systems should have their storage logically isolated from other systems that are not part of the BCS. At a networking layer, there should be no communications channels that allow the BCS to talk to any other system that is not controlled. At a virtual machine level, there should be logical isolation between VMs. As you “look down” through the computing stack, you should only see interface points that are controlled and locked down to a least-privilege position.

Logical isolation does not mean complete isolation. It means that only known, controlled communications can occur between a system and anything outside of its Logical Isolation Zone, and that all other communication is blocked. Serial communications such as RS-232 or RS-485 are logically isolated communications methods as well. These types of communications move data from the TX pin on one end of a cable to the RX pin on the other end of the cable. There is no addressing scheme or routing/firewall capability, so it meets the intent of logical isolation.

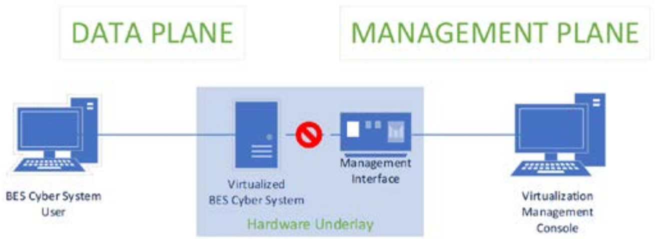
Management and Data Planes and CIP-005 R3

As the SDT considered virtualization, it identified a risk though not unique to virtualized infrastructures, is amplified by it. As virtualized servers, networks, switches, firewalls, and storage are logical constructs, controlling access and communications to the management plane of these systems becomes imperative. Access to the management plane (interface/console/etc.) allows a user to create, modify, or delete these objects or entire infrastructures from one place, or move objects from one zone or network to another. Administrative level or “management plane” access to the hypervisors is therefore absolutely critical to the security and reliability of the hosted systems and must be brought into the scope of CIP standards if hosting BES Cyber Systems.

Another example from a networking perspective is virtual LANs (VLANs) which are a method of logical isolation that can be used to meet CIP-005 R1. However, such logical isolation is critically dependent upon proper configuration of the isolation and management of access to those logical controls within the management plane of the switch or other network device. CIP-005 R3 brings that management plane of the switch into scope of the CIP standards, requiring that entities restrict access to the management functionality of these systems and isolate that access from the data plane (the normal, operational, non-administrative access).

Examples of this separation of the management plane and data plane can be accomplished in several different ways:

- A hypervisor can put its management interface IP address on a physical port or in a logical interface connected to a VLAN that is trunked to an upstream switch.
- Many hardware vendors include "integrated lights-out" or dedicated management interfaces that allow you to power on/off a cyber system.
- Physically isolated out-of-band network for management interfaces.
- Logically isolated out-of-band network (where logical constructs like VLAN, VXLAN, MPLS, VRF's (logical routers) are used to maintain logical isolation)



"Super-ESPs", CIP-005 R1.2, and the 4.2.3.3 Exemption

One of the issues with the ESP construct carried forward into the logical isolation model is the situation where entities have BES Cyber Systems that include components at separate locations. For example, if an entity has a need to replicate data at high speed between two databases in two different geographic locations to improve the resilience and reliability of BES Cyber Systems, the entity may have issues with the 4.2.3.2 exclusion in the standards that exempts the network and communications gear that is "between discrete ESPs." If this replication protocol is not a routable protocol, then no ESP can be created. The entity needs to be able to have a "Super-ESP" that can span more than one location.

The ESP model, along with the 4.2.3.2 exclusion within the CIP standards applicability does not lend itself to this construct. As technology evolves, there will be many more instances where a BES Cyber System may need to span locations. Another example could be the protection of a Transmission line consisting of digital devices at each end of the line with an IEC 61850 high speed network between them. This type of system, even with its components located in two geographically separate substations, can be shown to be logically isolated from other systems. The issue is that the 4.2.3.2 exclusion for limiting the scope of the involved communications gear between the sites does not apply. It is no longer "between" two ESP's or two logical isolation zones but is now completely "inside" a single BES Cyber System or a single logical isolation zone. Traditionally this situation could be addressed by installing an EAP at each site as an ESP boundary that would then allow the communications equipment between the sites to be subject to the exemption. There are issues however, such as:

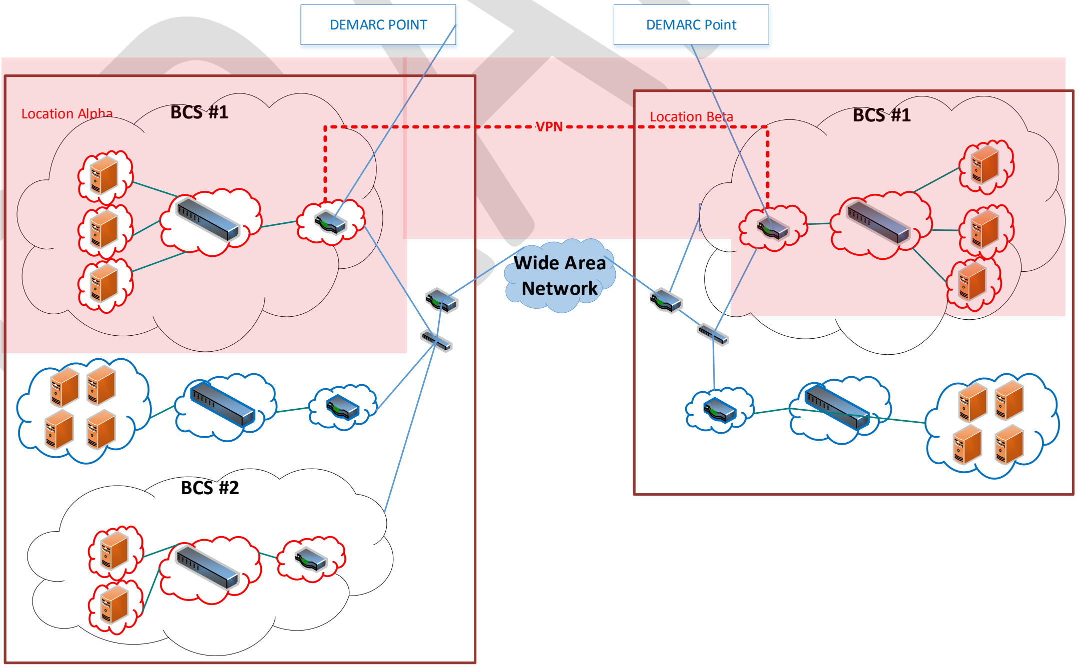
- Installing a firewall at each end of an essentially point to point circuit with rules allowing devices at either end to talk to the other adds complexity, single points of failure, and provides little security benefit.
- Some of these scenarios are extremely time sensitive and the devices need to communicate at very high speed to perform their asset protection function. Going through layers of security could cause latency and reliability issues that could hamper the asset protection function of the system.

This ‘Super ESP’ construct has been addressed with a new exclusion and a new requirement part in CIP-005 R1. The new exclusion in 4.2.3.3 allows communication networks and data communication links used by an isolated BES Cyber System that spans more than one geographic location to be exempt from the standards. The new R1.2 in CIP-005 pairs with this exemption and requires that the data over this exempted communication be protected to preserve its integrity and confidentiality, with the exception in R1.2 for those time sensitive protection functions.

“SUPER-ESP” EXCLUSION

Entity has 2 BCS with “BCS 1” having components in two locations. A VPN has been established between the components of BCS 1 at each location to logically isolate that BCS across the locations. Further logical isolation occurs at other touch points to other networks or out of scope systems. The entity chooses an appropriate demarcation point at each location and the networks between those points are excluded unless CIP-012 is applicable.

(NOTE: Red Cloud icons only denote some form of logical isolation for the BCS, Blue Cloud icons denote some form of logical isolation for the non-BCS)



External Routable Connectivity and Interactive Remote Access

External Routable Connectivity (ERC) is used in the CIP standards for different purposes, including:

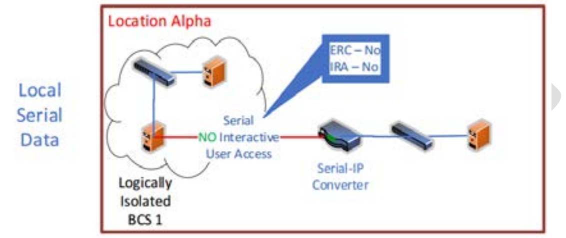
1. Establishing when EAPs are required
2. Limiting scope of ~38 requirement parts to those locations that have a high enough level of remote connectivity to support the requirement

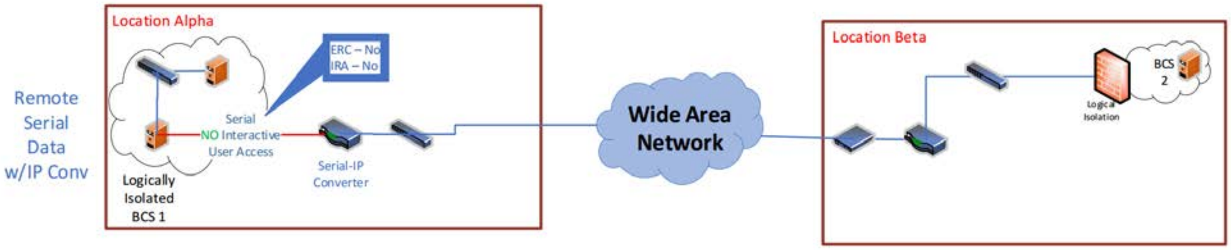
The move to the more objective-based logical isolation concept shifts the requirement to an obligation that shows the system is logically isolated with controlled communications at any interface point or shared infrastructure. This can be accomplished without dictating any architecture or access control method. ERC is still needed as a scoping mechanism due to the vast scale of systems and their components within a geographically distributed BES. Many requirement parts should be scoped based on whether the system has ERC for the following reasons:

- The risk is increased for systems with ERC. The requirement should apply to those systems with an increased attack surface and risk due to their connectivity/accessibility.
- Locations that have legacy connectivity such as non-routable serial leased circuits should not have to increase their level of remote connectivity and attack surface to meet security requirements. For example, it would not be advisable to put in an IP network into a site to get SNMP traps out for alerts if a serial circuit with reduced attack surface is all that is needed for operations.

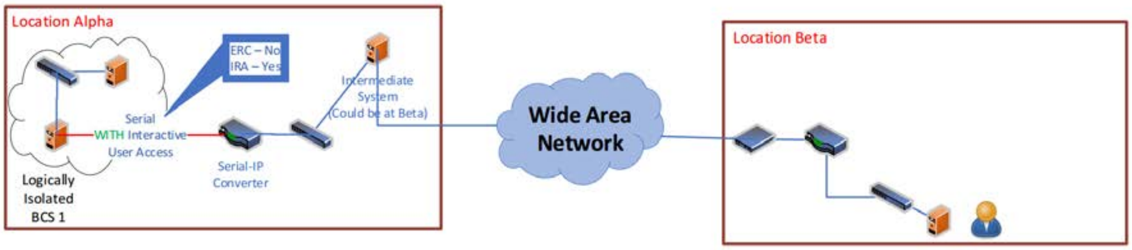
One issue with the ERC definition from the V5TAG transfer document has been that of BES Cyber Assets (BCA) that only speak non-routable protocols over a serial port. These BCAs are not in an ESP and therefore can be considered to not have ERC because it is defined in terms of an "associated ESP." These BCAs, however, can have Interactive Remote Access through an upstream serial-to-IP conversion. The SDT has kept ERC as-is with only conforming changes in order to not disrupt its scoping function as noted above. However, the IRA definition has been modified so that a device with only a serial, non-routable connection could now have IRA and be subject to CIP-005 R2. Appropriate controls (CIP-005 R2) are now required for these Interactive Remote Access sessions without regard to ERC.

The following diagrams show different scenarios and whether ERC and/or IRA exist in the situation.

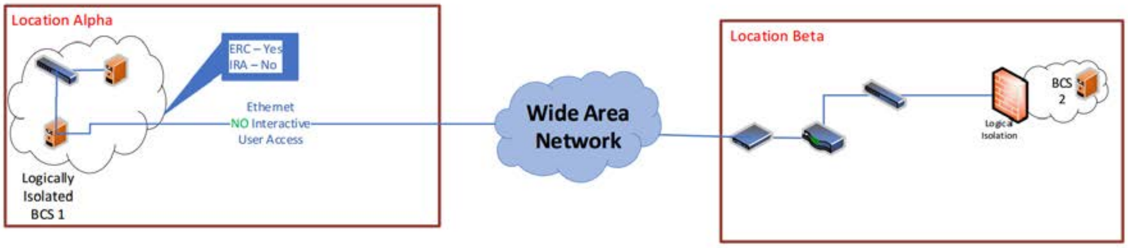




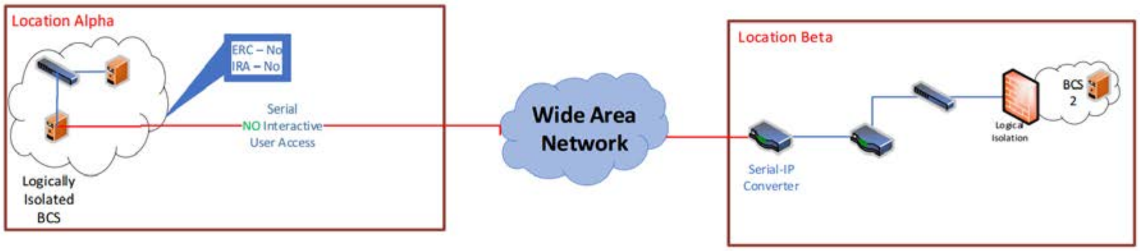
Remote Serial Access



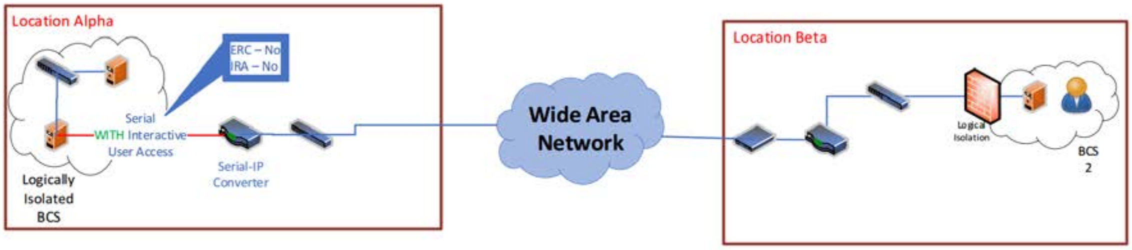
Remote Routable Data



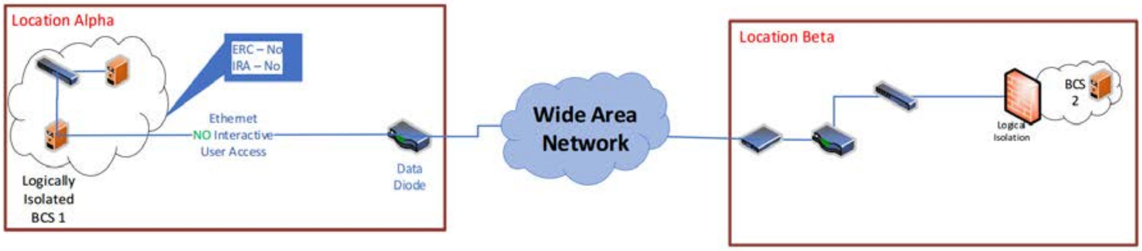
Remote Serial Data

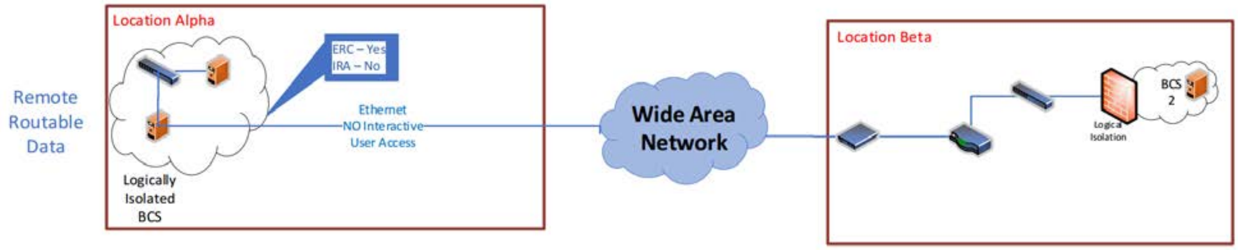


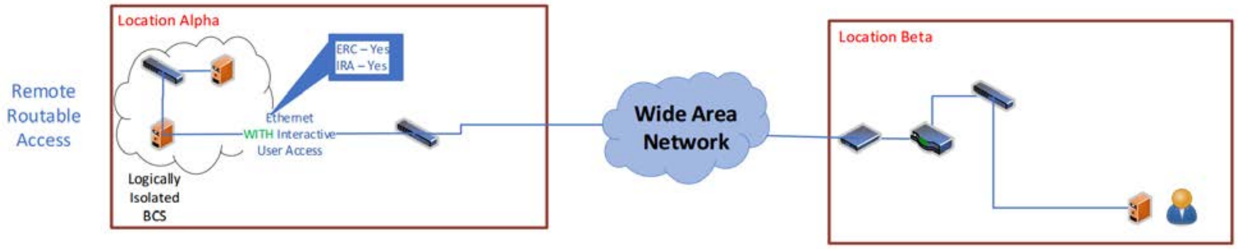
Remote Serial Access From Another BCS



Diode







EACMS Changes to EACS and EAMS

As technologies and attacks have advanced and become more complex, entities are becoming more interested in partnering with outside and government security services. These includes services like NERC's Cyber Security Risk Information Sharing Program (CRISP), Cybersecurity for the Operational Technology (OT) Environment (CYOTE), and those of other external security services and internal monitoring centers. Going forward, these types of service and providers will become more cloud based. Security service providers have visibility into emerging threats and trends that come through their extensive collections of information. Analysis of this information can then be shared more broadly, improving the overall cybersecurity posture and reliability of the BES through early detection of compromise and the ability to monitor for threats and indicators of compromise (IOCs) at machine speeds.

Under the current body of CIP Standards, using the types of services that include electronic access monitoring data (not involved in the actual control of electronic access) may bring all Cyber Assets involved into scope as an EACMS. This may discourage or even preclude entities from using these services based on the cyber asset level requirements of an EACMS. These limitations affect personnel, physical security, patching, baselines, and other requirements that focus on a Cyber Asset. Entities may also be discouraged from providing and correlating security events across enterprise and control networks, even though most cyber-attacks against control systems today enter through business networks. There is great value in correlating security events seen across enterprise and OT networks that may be discouraged or precluded through the "M" in EACMS growing to include much an enterprise's other monitoring only Cyber Assets.

The cyber systems that do perform electronic access control will remain as they are today in the standards. Those cyber systems, such as firewalls and routers with ACLs and other systems that do perform access control and actively protect the networks to which BES Cyber Systems are connected should not change. However, the monitoring and logging aspect of EACMS presents a different though lesser risk. The creation of two different defined terms recognizes this. EACS represents those systems that do control electronic access and will essentially be a drop-in replacement for today's EACMS.

CIP-007-7 Technical Rationale

Project 2016-02: Modifications to CIP Standards

CIP-007-7 R1

The original technical rationale for CIP-007-6 Requirement R1 described the existence of Requirement R1 as being needed "…to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports." The reasoning remains the same for Requirement R1 with the new objective language "to mitigate the risk posed by uncontrolled logical and physical connectivity." The changes in Requirement R1 language continue the move from Cyber Asset up to the BES Cyber System and supports the secure configuration implemented within CIP-010-3 Requirement R1.

CIP-007 Requirement R1 is intended to limit the ability of an attacker to move laterally throughout the secure environment.

CIP-007 R1 Part 1.1

The move to logical connectivity supports the proliferation of additional connectivity options found in modern technology stacks such as virtualization. With SAN connectivity over Fiber Channel delivering storage to virtualized systems without the use of IP or a "network," the limitation of network based controls becomes more clear. Additionally, the connectivity of a local hypervisor based configuration manager to the VM likewise does not go through a "network accessible port" in the strict sense.

By moving the control to "logical connectivity" the requirement can be applied in both the original "logical network accessible port" model as well as in the virtualized system to apply access controls to the network and storage "fabric" and hypervisor supporting a virtualized BES Cyber System.

CIP-007-7 R2

The original technical rationale for CIP-007-6 Requirement R2 included the intent "to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets." This intent was determined to logically fit within the intent of CIP-010-2 R3 associated with vulnerability assessment and management. Accordingly, the SDT moved the related requirements from CIP-007-6 Requirement R2, with modifications supporting virtualization, to CIP-010-4 Requirement R3 Parts 3.5 and 3.6.

The SDT is including a replacement requirement related to controlling software that is allowed to execute on applicable BES Cyber Systems with the inclusion of the objective "to mitigate the risk posed by unmanaged software". This clarifies one of the implied requirements of the original CIP-007-6 Requirement R2 for a list of software, and supports the secure configuration implemented within CIP-010-4 Requirement R1.

CIP-007 R2 Part 2.1

The inclusion of the objective in Requirement R2 Part 2.1, “to allow only essential software execution” further clarifies the intent of CIP-007 Requirement R2 to limit what software can execute on a system. This requirement helps ensure that entities control software execution, which limits the attack vectors, and limits the scope of required software vulnerability management efforts in CIP-010-3 R3 Parts 3.5 & 3.6.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-010-4 Technical Rationale

Project 2016-02

Requirement R1

The SDT proposes to retire the CIP-010 R1, Part 1.1 baseline configuration requirement and introduce a new related definition describing a Secure Configuration. This Secure Configuration consists of the security control methods implemented to comply with other requirement parts contained in CIP-005, CIP-007, and CIP-010. To avoid creating a long list of requirements in either the definition or in CIP-010 R1 itself, it states within each pertinent requirement part that it is part of the Secure Configuration. This was done by including the statement "The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system."

One reason for retiring the baseline configuration is that while the baseline requirement is applicable to BES Cyber Systems, its implementation tended to drive Responsible Entities into creating a 1-to-1 relationship between BES Cyber Assets and BES Cyber Systems. This was partially due to uncertainty in how to document a baseline where multiple disparate BES Cyber Assets were included in a single BES Cyber System. The question was how to reference multiple Operating Systems on a single BES Cyber System. On a list of installed software, what indicates that the software may be installed only on a single virtual machine or that there may be multiple copies of it across multiple virtual machines? These challenges didn't exist in a 1 to 1 BCA-BCS relationship. That relationship effectively limited the adoption of the system approach and ignored a fundamental aspect in the application of virtualization and emerging technologies to the CIP standards.

The existing baseline configuration serves as a list creating a requirement for implementing change control processes for these configuration items. The proposed Secure Configuration definition then ensures that this scoping for the change control process includes required security controls implemented to protect the BES Cyber System. This is an expansion over the scope of items that must go through change control under the existing CIP standards. The rationale for expanding the scope comes from risks associated with virtualization and emerging technologies. Specifically in virtualization, a few clicks can dramatically change your system architecture and the resources on which your applications are executing. Given this unique risk, change control for security settings was an essential element for mitigation. While this risk is greater for virtualized systems, the risk of inadvertently modifying security controls also exists in physical and traditional systems. For these reasons, this expanded scope should apply to all Medium and High Impact BES Cyber Systems.

Moving the baseline configuration from a requirement to a Secure Configuration definition should reduce the administrative overhead required to comply with CIP-010. Along with creating the Secure Configuration definition and removing the requirement to maintain a list of baseline configurations for all BES Cyber Systems, there is a new proposed requirement in CIP-007 (specifically the new CIP-007 R2) and modifications to CIP-007 R1. By creating related controls and removing list-making requirements, these changes collectively provide an increase in security and reduce the CIP standards' administrative overhead.

Only conforming changes based on newly modified definitions and the new Secure Configuration concept were made to the remaining requirement parts in CIP-010 R1.

Requirement R2

There are only minor adjustments to Requirement R2. The primary modification was to split the requirement into two parts based on the 'monitor' and 'investigate' obligations that were specified in Requirement R2. Changes to the structure of the requirement part added some examples of how to perform configuration monitoring. Input from regulatory staff indicated that they had observed some Responsible Entities implementing configuration monitoring, but not in an effective manner. The examples provide additional context on how to effectively meet the security objective of this requirement part.

Requirement R3

The primary change made to R3 was the addition of the vulnerability management (formerly patch management) requirement that was previously located in CIP-007 R2. The relocation of the requirement better acknowledges that patching is one component of an overall vulnerability management program that includes ongoing analysis, mitigation, and periodic vulnerability assessments. It is generally recognized that the existing patch management requirement is very prescriptive. As part of this prescriptiveness, the assessment of risk, a fundamental element of vulnerability management, was left out entirely – all vulnerabilities were treated exactly the same. In a virtualization context, a risk-based view of vulnerability management becomes even more important. It is essential that the requirements provide enough flexibility to recognize that some patches are critical and must be dealt with urgently while others could reasonably wait for implementation or may be better mitigated through other means.

Entity Identified Timeframes

Modifications to CIP-010 propose a new concept regarding the timeframes that currently prescribe actions required at least every 35 days or similar. These prescriptive requirements, while useful reference points for completing certain tasks, may also have a number of unintended consequences. Primarily, these prescriptive timelines discourage any risk analysis to determine when activities should be completed. In certain instances, the risk is so great that 35 days may be too long. In others, 35 days is much too short. A prescriptive 35-day requirement prevents Responsible Entities from allocating their resources to address the highest risks first. Consider the patching requirement. Responsible Entities are currently required to identify and evaluate security patches at least every 35 days. Some equipment has never had an applicable security patch released, while some software may regularly have patches released monthly or more frequently. The criticality of the patch is also not considered in today's requirements. Current requirements prescribe that we treat all of those examples the same. This is an increasingly important topic in the context of virtualization. In virtualization, a single vulnerability in the underlying infrastructure may impact all of your systems. This could be through a single patch causing all of your systems to fail, or a single vulnerability that could create security risk across all of your systems.

In either case, virtualization requires extra care from both security and functional perspectives.

Responsible Entities need greater flexibility regarding timelines for when activities are performed. In particular, additional risk analysis is needed when determining how to proceed. CIP-010 permits Responsible Entities to perform a risk analysis to determine the most appropriate timeframe for their unique environment. There are several forms of this language in CIP-010 depending on the objective of the requirement and the analysis that needs to take place. Some examples include:

> *From Part 1.1:* "The process requirements of Parts 1.1.1 through 1.1.4 and timeline are based on the analysis of the risk to BES reliability and the risk posed by the change to the system(s)."
>
> *From Part 2.1:* "The process requirements of Part 2.1 and timeline are based on the analysis of the risk to BES reliability and the impact rating of the applicable system(s)."
>
> *From Part 3.6:* "The plan for Part 3.6 must include the timeline for mitigating the software vulnerability based on the analysis of the risk posed by the software vulnerability to the applicable systems."

Each example specifies what the risk analysis needs to include. For example, in Part 3.6, it is important to evaluate the risk of the specific vulnerability when determining how quickly it needs to be mitigated. In Part 1.1, timelines should be based on the risk posed by the change itself.

These changes are not entirely backwards compatible. This flexibility, however, should increase security by shifting the focus to risk-based vulnerability management and should reduce administrative compliance violations when the risk of taking an action does not change from day 35 to day 36.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Announcement

2016-02 Modifications to CIP Standards Virtualization

Informal Comment Period Open through December 18, 2018

Now Available

An informal comment period for **Virtualization Updates for CIP-004, CIP-005, CIP-006, CIP-007, CIP-010, and Associated Definitions** is open through **8 p.m. Eastern, Tuesday, December 18, 2018**.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience Issues using the SBS, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The drafting team will review all responses received and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Standards Developer, Jordan Mallory (via email) or at 404-446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization Updates for CIP-004, CIP-005, CIP-006, CIP-007, CIP-010, and Associated Definitions
Comment Period Start Date:	11/2/2018
Comment Period End Date:	12/18/2018
Associated Ballots:	

There were 76 sets of responses, including comments from approximately 199 different people from approximately 132 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The proposed BCS definition no longer relies on the term Cyber Asset. The SDT asserts that the proposed BES Cyber System definition describes the BCS adequately without the use of the word “programmable” in the definition. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

2. The SDT asserts that the proposed Cyber Asset definition provides clarity around virtual hardware. (Cyber Assets revised definition: Programmable electronic devices, including the physical or virtual hardware, software, and data in those devices.) Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

3. The SDT asserts that the term Cyber Asset should continue to be used within the NERC Glossary of Terms for: Removable Media and Transient Cyber Asset. Due to the nature of that type of hardware, these devices do not lend themselves to the systems approach. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

4. The SDT is proposing to retire EACMS and develop two new terms: EACS and EAMS. These terms will allow changes within the applicability for the monitoring portion to allow third party monitoring systems. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

5. The SDT realized through the process of splitting EACMS that the same considerations apply to PACS, which will allow changes within the applicability for alerting and logging (PAMS is not reflected within the applicability section at this time). The SDT is considering splitting the PACS term into PACS and PAMS to allow third party monitoring or event correlation to be performed without carrying the PACS classification. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

6. The SDT is proposing to move away from the more prescriptive ESP/EAP model to logical isolation through the higher level objectives provided by the BES Cyber System concept and its Logical Isolation Zone. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

7. The SDT is considering taking qualitative language out of the Intermediate System definition and using it to clarify requirements. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

8. The SDT is considering changes to the ERC and IRA definitions to address V5TAG issues (see the CIP-005 Technical Rationale document for detailed information). ERC will have conforming changes only and will continue its use as a scoping mechanism. The proposed modifications to IRA will apply to certain non-routable to routable protocol conversion scenarios. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

9. To the extent possible, the SDT intends its modifications to permit approaches to compliance that are “backwards compatible” with compliance approaches within the currently approved versions of the CIP standards. (Notable exceptions include CIP-005 R3, CIP-007 R2, and Secure Configurations – CIP-010). Do you agree the modifications are backwards compatible? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

10. The SDT has not yet determined a proposed timeframe to include in the Implementation Plan. How long would you as an entity need to implement the proposed modifications? Please provide your implementation timeframe and justification for why that amount of time would be needed.

11. The SDT is proposing conforming modifications to CIP-004. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. Modifications related to CIP Exceptional Circumstances

b. Use of newly proposed terms EACS and EAMS in the Applicable Systems column

c. Addition of PCS to the Applicable System column for Parts in CIP-004 to mitigate security risks associated with individuals not needing authorization or PRAs when granted access to systems inside the Logical Isolation Zone

12. The SDT is proposing modifications to CIP-005 (see the CIP-005 Technical Rationale document for detailed information). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The replacement of the ESP concept with Logical Isolation Zone (LIZ).

b. Is the backward compatibility clear as existing ESPs and EAPs move to the new LIZ concept?

c. The addition of the 4.2.3.3 exemption in the standard along with the addition of Requirement part R1.2 to address the V5TAG concern of “Super ESPs” or single networks within or between BES Cyber Systems that span more than one geographic location.

d. As differing forms of shared infrastructure come into play with virtualization, Requirement R3 has been added to include the management plane and its isolation controls as a part of the CIP standards. Is this concept clearly and widely understood?

13. The SDT is proposing conforming modifications to CIP-006. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. Modifications related to CIP Exceptional Circumstances

b. Use of newly proposed term EACS in the Applicable Systems column

14. The SDT is proposing modifications to CIP-007 (see the CIP-007 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The SDT is proposing adding the security objectives throughout the Requirements in CIP-007. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?

b. The SDT is proposing the security objective in CIP-007 R1, “to mitigate the risk posed by uncontrolled logical and physical connectivity". Do you agree that the modifications to CIP-007 R1 Part 1.1 fulfill this security objective for systems where connectivity is not limited to TCP/IP port service combinations, as in virtualized systems and SAN based storage?

c. Do you agree that the modifications to CIP-007 R1 Part 1.1 add necessary flexibility to fulfill the security objective of CIP-007 R1 for virtualized systems and provides a degree of future proofing?

15. The SDT is proposing modifications to CIP-010 (see the CIP-010 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The SDT is proposing adding the security objectives throughout the Requirements in CIP-010. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?

b. The SDT is proposing to modify the referenced baseline configuration from CIP-010-3 R1 Part 1.1 to a ‘Secure Configuration’ which is made up of the implemented controls that fulfill requirements within CIP-005 and CIP-007. Do you agree that this set of controls supports managing change under CIP-010 R1 Part 1.1?

c. The SDT is proposing to modify the current CIP-007 R2 requirements and move them to CIP-010 R3. The SDT believes that the software vulnerability management found within this set of requirements fits logically within the security objective of CIP-010 R3 “to mitigate the risk posed by system vulnerabilities” and has moved it there. Do you agree?

d. The SDT is proposing CIP-010 R3 Parts 3.5 and 3.6 to replace the current CIP-007 R2 Parts 2.1 – 2.4. Do you agree that the proposed CIP-010 R3 Parts 3.5 and 3.6 offer the additional flexibility needed when implementing virtualized systems that can be dormant for a period, and for which security patches have become available?

16. Provide any additional comments for the SDT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1,3,5	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Santee Cooper	Chris Wagner	1,3,5,6		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Travis Bryan	Santee Cooper	1,3,5,6	SERC
					Shedrick Snider	Santee Cooper	1,3,5,6	SERC
					Wanda Williams	Santee Cooper	1,3,5,6	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO

					Brad Parret	Minnesota Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent ISO	2	MRO
Public Utility District No. 1 of Chelan County	Davis Jelusich	1,3,5,6		Public Utility District No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC
PPL - Louisville Gas and Electric Co.	Devin Shines	3,5,6	RF,SERC	Louisville Gas and Electric Company and Kentucky Utilities Company	Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					JULIE HOSTRANDER	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
Great Plains Energy - Kansas City	Douglas Webb	1,3,5,6	MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO

Power and Light Co.								
Lincoln Electric System	Eric Ruskamp	1,3,5,6		LES	Eric Ruskamp	Lincoln Electric System	6	MRO
					Dan Pudenz	Lincoln Electric System	1	MRO
					Jason Fortik	Lincoln Electric System	3	MRO
					Kayleigh Wilkerson	Lincoln Electric System	5	MRO
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
ACES Power Marketing	Jodirah Green	6	NA - Not Applicable	ACES Standard Collaborations	Eric Jensen	Arizona Electric Power Cooperative, Inc	1	WECC
					Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Greg Froehling	Rayburn Country Electric Cooperative, Inc.	3,6	Texas RE

					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Amber Skillern	East Kentucky Power Cooperative	1,3	SERC
					Ginger Mercier	Prairie Power, Inc.	1,3	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Southwest Power Pool, Inc. (RTO)	Kimberly Van Brimer	2	MRO	SPP Member Group	Matt Harward	SPP	2	MRO
					Louis Guidry	Cleco	1,3,5,6	SERC
					Joe Gatten	Xcelenergy	1,3,5,6	MRO
Manitoba Hydro	Mike Smith	1,3,5,6		Manitoba Hydro	Yuguang Xiao	Manitoba Hydro	5	MRO
					Karim Abdel-Hadi	Manitoba Hydro	3	MRO
					Blair Mukanik	Manitoba Hydro	6	MRO
					Mike Smith	Manitoba Hydro	1	MRO
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC

Lakeland Electric	Patricia Boody	1,3,5,6		Lakeland CIP	Jim Howard	Lakeland Electric	5	FRCC
					Larry Watt	Lakeland Electric	1	FRCC
					Paul Shipps	Lakeland Electric	6	FRCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion and NYPA	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Michael Jones	National Grid	3	NPCC
					Sean Cavote	PSEG	4	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					David Kiguel	Independent	NA - Not Applicable	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Caroline Dupuis	Hydro Quebec	1	NPCC

					Chantal Mazza	Hydro Quebec	2	NPCC
					Michael Forte	Con Edison	1	NPCC
					Laura McLeod	NB Power Corporation	5	NPCC
					Nick	Kowalczyk	1	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					John Hastings	National Grid	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Sofia Gadea-Omelchenko	Con Edison	5	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
PSEG	Sean Cavote	1,3,5,6	FRCC,NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	NPCC
					Karla Barton	PSEG - PSEG Energy Resources and Trade LLC	6	RF

					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co.	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co.	1	RF
Lower Colorado River Authority	Teresa Cantwell	1,5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Associated Electric Cooperative, Inc.	Todd Bennett	1,3,5,6		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC
					Walter Kenyon	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri	1	SERC

						Electric Power Cooperative		
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The proposed BCS definition no longer relies on the term Cyber Asset. The SDT asserts that the proposed BES Cyber System definition describes the BCS adequately without the use of the word “programmable” in the definition. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
It’s clear, but concern about how it will be audited. Concerns that there is not clear tie to an impact to the BES and its replaced with only the impact to a BES Facility.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
It’s clear, but concern about how it will be audited. Concerns that there is not clear tie to an impact to the BES and its replaced with only the impact to a BES Facility.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
IESO agrees with the new BCS definition. While this change may add additional assets/devices into the CIP program (via re-evalutation of CIP-002), the controls being used should remain the same.	
Likes 0	

Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Yes, however adding the 15-minute requirement to BCS might change the composition of our Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Yes, however adding the 15-minute requirement to BCS might change the composition of our Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA. Please see our response to Question 16, below, for a summary of our comments and position regarding the changes and approached proposed herein.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

APPA does not believe the removal of “programmable” adequately scopes the applicable device types with the current definition. APPA believes that the new definition would include devices that have been previously excluded, such as electro-mechanical relays, since “any combination of” would include hardware only, and there is no scope placed on the hardware to eliminate these devices.

In any case, because “programmable” remains in the legacy definition of “cyber asset,” the issue about its meaning—to the degree that remains an issue—has not been eliminated.

Additionally, APPA does not believe the proposed BES Cyber System definition describes the BCS appropriately. The new definition is attempting to combine many definitions into one. Public power recommends using the language below:

A BES Cyber System includes any combination of programmable hardware (including virtual hardware), software (including application virtualization), and data, where:

1. It/they performs one or more reliability tasks; and

2. If rendered unavailable, degraded, or misused, the situation would result in adverse impact to one or more BES Facilities within 15 minutes. Redundancy is not a factor, in the sense of considering the activation of different, redundant BES Cyber Systems.

The language “regardless of redundancy,” as used in the proposed definition, is unclear. Does “regardless of redundancy” apply to all items (hardware, software, and data)? It seems that the redundancy being introduced is intended to address the BES Cyber Asset definition, but the language structure makes this difficult to decipher. We understand that redundancy in determining systems is based on the language in CIP-002-5.1a as it relates to Real-Time Operations:

“This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.” In this regard, revisions to the core BCS definition will require some Entities to re-work their CIP-002-5.1a process to address the Real-time Operations decision at a different point in the process to identify BES Cyber Systems.

The recommended revised definition above attempts to incorporate these concepts.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6

Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST.

The current BCS definition has the potential to increase the scope / applicability of the CIP standards. The BCS definition should include a reference to Cyber Asset definitions, and further define what is meant by hardware, software, data, etc. As currently written, it seems “hardware” that do not satisfy the definition of Cyber Asset could be brought in under the BCS definition.

In addition, any changes to existing terminology or definitions should provide a security benefit considering the extent of administrative changes that will be required to implement these changes (policies, procedures, tools, asset management systems, device labeling, updated training materials, implementing staff training, etc.). It seems the current proposed change does not provide a security benefit.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC does not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). This proposed change would require entities to re-evaluate what is in scope under CIP-002 and could cause non-programmable devices to be included. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs. SMEC is concerned that this magnitude of change to the CIP standards would be too disruptive to non-virtualization compliance.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes that for the sake of avoiding arguments during audits, the word, “programmable” should be retained. Suggest rewording: “A programmable combination of physical and/or virtual hardware, software and data, performing or supporting one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes. Redundancy shall not be considered when identifying BES Cyber Systems.”

Likes 0	

Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	No
Document Name	
Comment	
We believe the the new definition of BES Cyber System should contain the term Cyber Asset, like: "Any combination of Cyber Assets, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes." Additionally, we believe the new definition, without the use of "programmable" will bring into scope electronic devices that are not capable of being updated and have no means to update the software or firmware within them (not field updateable). These devices currently do not meet the “programmable” electronic device definition and are thus out of scope for NERC CIP.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The proposed definition of BCS does not address the issues and interpretations that surfaced by not having a definition of programmable.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI:	

"EEI does not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). While we understand the SDT's desire to move from the current asset focused model to a systems approach, the changes being proposed within the body of revised and retired definitions appears to go well beyond what we understand was intended within the currently approved SAR. EEI believes that the SDT should retain the defined terms "BES Cyber Assets (BCA)" and BES Cyber System (BCS) as currently written. We also believe that given the proposed revisions made to the term "Cyber Asset," which clarify that physical or virtual hardware, software and data are allowed, obviates the need to revise the other definitions."	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	No
Document Name	
Comment	
Some concern that "Any combination of hardware.." with out programmable could lead to more confusion about what specific devices are or are not in-scope.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
Exelon does not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). While we understand the SDT's desire to move from the current device-focused model to a systems approach, the changes being proposed involve fundamental definitions and appear to go well beyond what we understand was intended within the currently approved SAR. The proposed change represents a major overhaul of the CIP Standards, including impacts on CIP-002 methodologies, assessment methods, and many current CIP Program processes and procedures. These changes would be better addressed in a separate and comprehensive major CIP version upgrade effort.	
Likes 0	
Dislikes 0	
Response	

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 1.

Likes 0	
Dislikes 0	

Response

Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6

Answer	No
Document Name	

Comment

Some concern that “Any combination of hardware..” with out programmable could lead to more confusion about what specific devices are or are not in-scope.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No
Document Name	

Comment

Covering all items without consideration of the difference between programmable and non-programmable devices introduces significant complications for physical security and for configuration management. Should an auditor independently determine that communications cabling, electrical wiring, or non-programmable devices such as electro-mechanical relays are part of the system, the scope of CIP-006 could grow drastically. This could have a tremendous impact on medium impact generation assets.

While “programmable” or a suitable variation of the term is needed, the issues with the current non-definition of programmable need to be addressed. The definition is based on programmable, the various types of programmability needs to be addressed: (1) Remotely programmable; (2) requires physical access and interruption of operation to change device programming; Electromechanical devices (including devices such as electromechanicable breakers and physical hardware such as communications cabling and electrical wiring).

.

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	

Comment

CHPD disagrees with the removal of Cyber Asset from the definition. The new language will expand the current scope of the definition by bringing any electro-mechanical BES device into scope due to “Any combination…” language and the lack of a tie to the “Programmable” term defined in the Cyber Asset definition.

CHPD suggests using the new Cyber Asset definition (already scopes virtual systems) with the following BES Cyber System definition:

“A combination of one or more Cyber Assets performing one or more reliability tasks, including redundant members that support a reliability task, that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.”

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy does not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). While we understand the SDT’s desire to move from the current asset focused model to a systems approach, the changes being proposed within the body of revised and retired definitions appears to go well beyond what we understand was intended within the currently approved SAR. In addition, the revisions will create a significant change to existing processes, and documentation, due to revising the foundation of the identification of CIP Assets.

With the removal of the term, Cyber Asset, the SDT will be removing the necessary tie to BCS, and in turn, revising the current filtering system that Entities use to identify their CIP Assets. Additionally, with the removal of BCA, there is no explicit language within CIP Glossary Terms that address non-programmable devices as non-CIP applicable assets.

NV Energy believes that the SDT should retain the defined terms “BES Cyber Assets (BCA)” and BES Cyber System (BCS) as currently written. We also believe that given the proposed revisions made to the term “Cyber Asset,” which clarify that physical or virtual hardware, software and data are allowed, obviates the need to revise the other definitions.

NV Energy also believes that the revisions to the definition provide no improvement to reliability and security, and mainly address possible confusions found during auditing of the standards.

Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Please clarify “regardless of redundancy” with respect to the “combination of hardware, software, and date.” Redundancy in this context appears to relate more to the BCA definition. With respect to redundancy, as stated in CIP-002-5.1a, relative to Real-Time Operations, “…redundancy does not mitigate cyber security vulnerabilities.” Revisions to the BCS definition may cause entities the burden of redefining and modifying their classification process, as well as subsequent processes/workflows that are intertwined. Not all BCS include virtualization. The retirement of the use of the term BCA affects how audit evidence in currently proposed in “CIP Version 5 Evidence Request v2.0”. In v1.0, there were tabs for both virtual systems and BCS, in v2.0, both are eliminated. How will device sampling be handled?	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
By removing the term “programmable” and the tie to “BES Cyber Asset” (which removes the tie to “Cyber Asset”), the term BES Cyber System does not provide a clear means to exclude devices that are hardware with built-in programmable read-only memory (PROM) or can only be interacted with through a push-button interface (or similar physical interaction). Including these devices in CIP cyber security scope creates administrative burden with no clear benefit to cyber risk. Previously, these could be excluded by an entity using internal definition/clarification of “programmable” to indicate programmable through an electronic interface and without disassembly of the device (i.e. replacing a PROM chip). Suggested options: Cyber Asset: A programmable electronic device, including the hardware (physical or virtual), software (including application virtualization), and data in these devices. BES Cyber System: Any combination of Cyber Assets, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused, would result in adverse impact to one or more BES Facilities within 15 minutes.	
Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Please see Texas RE’s response to #3.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Comments: PacifiCorp’s approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

Not using Cyber Asset in the definition of BES Cyber Systems removes the necessary ties between the two terms. The terms should be used as a filtering mechanism to scope the assets subject to the CIP standards. Starting with Cyber Asset being the largest population of devices, followed by a filtering process to determine whether the Cyber Assets are part of a BES Cyber System. PAC suggests adding either Cyber Asset or programmable into the proposed BCS definition.

Option 1: BES Cyber System - Any combination of [Cyber Assets, that includes] hardware (including virtual hardware), software (including application virtualization), and data, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.

Option 2: BES Cyber System - Any combination of [programmable electronic devices, that includes] hardware (including virtual hardware), software (including application virtualization), and data, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

The new definition expands the scope of devices that would fall into CIP regulation if the Cyber Asset term is removed by removing the BCA component. Currently only programmable electronic devices are in scope. The new definition would bring into scope electronic devices that are not capable of being updated; no means to update the software or firmware within them (not field updateable). These devices currently do not meet the "programmable" electronic device definition and are thus out of scope for NERC CIP.

The NSRF recommends leaving the BES Cyber Asset and, BES Cyber Systems definitions and accepting the proposed Cyber Asset definition. We feel this allows for virtualization and significantly reduces the documentation changes that would be required by the elimination of the BCA definition.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

We disagree with the proposed BCS definition. The NERC CIP requirements are generally device-centric, which are working well for both physical and virtual CIP Cyber Assets in registered entities' CIP compliance programs. In our virtual environment, we have no issue for continuously using the device-centric approach for the CIP compliance. For instance, we have identified the VM and SAN as a distinct virtual programmable device. CIP Version 5 previously introduced the concept of BES Cyber Systems to assist registered entities performing and documenting compliance actions by reducing the amount of required compliance documentation, and in some cases, to allow one BES Cyber Asset in a BES Cyber System to perform required actions on behalf of other BES Cyber Assets in the BES Cyber System. These BCA and BCS terms used in the registered entities' CIP compliance process today work fairly smoothly. In addition, the new term BES that breaks down from the Cyber Asset level to the hardware and software level is not manageable and auditable, and it would create additional identification workload that has no value for the registered entities. Based on the above rationale, there is no need for redefining the BCS from a compliance and security perspective. We disagree with the PCS definition for the same reason.

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
Due to the proposed retirement of the BCA definition and because the designation of the new Cyber Asset term is intentionally limited to TCA, Removable Media, and CIP-010 we believe the proposed BES Cyber System definition needs further clarification. As an example, the term “programmable” in the BCA definition currently excludes certain BCS Elements, such as Current Transformers [CT] and Potential Transformers [PT] for transmission protection BCS. Since these devices, if rendered unavailable, degraded, or misused, could cause failure of the host transmission protection BCS, the new definition of BCS could be interpreted to include all such nonprogrammable elements within a given BCS as part of the specific combination of hardware, software, and data.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Entities need guidance on what makes up a BCS. The term programmable gave sufficient guidance that cyber assets were of concern.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	

Comment

Reclamation does not support retiring the term BES Cyber Asset. Reclamation recommends the term BES Cyber Asset be retained and used as it is currently defined in all applicable definitions in the NERC Glossary of Terms.

Reclamation also does not support the proposed definition of BES Cyber System. Defining BES Cyber System without using the term “BES Cyber Asset” (to include the term “programmable”) could bring equipment like PTs, CTs, pressure sensors, temperature sensors, and other hardware devices for BES functionality into scope.

If the above recommendation is not adopted, Reclamation proposes the following definition of BES Cyber System:

BES Cyber System – One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.

Likes 0	
Dislikes 0	

Response

Joseph Pride - Trans Bay Cable LLC - 1 - WECC

Answer	No
Document Name	

Comment

Eliminating the word “programmable” blurs the line between a cyber asset and complex electrical or electronic hardware, such as non-programmable relays. It opens the door to enforcement on many more assets that don’t make sense, such as integrated appliances or complex semiconductor switching devices that do not have field-changeable firmware.

The important nuance provided by the word “programmable” is that it is possible for the executable code to be modified in the field, other than just changing settings in a faceplate menu. That makes the CIP Standards relevant as protections against the device being a target for attackers (BCS) or being reconfigured for use in an intrusion or attack (EACMS, PACS, PCA). There may be value in adding a defined term for “Programmable.” A possible definition could be “containing executable code, including binaries and scripts, that can be modified after manufacture or creation. This is an intrinsic characteristic, not a situational one, which does not change with respect to whether the end user connects, secures, removes, or blocks any access paths that can used to modify executable code. This does not include the ability to modify basic configuration data that are not executed sequentially as scripts, such as a setpoint or IP address.”

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	No
Document Name	

Comment

We do not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). While we understand the SDT's desire to move from the current asset focused model to a systems approach, the changes being proposed within the body of revised and retired definitions appears to go well beyond what we understand was intended within the currently approved SAR.

We believe that the SDT should retain the defined terms "BES Cyber Assets (BCA)" and BES Cyber System (BCS) as currently written. We also believe that given the proposed revisions made to the term "Cyber Asset," which clarify that physical or virtual hardware, software and data are allowed, obviates the need to revise the other definitions.

We recommend returning the "programmable" language to the BCS definition, as well as maintaining a definition of BES Cyber Asset as a component of the BCS. We believe these changes improve backward compatibility.

This proposed change ripples into CIP-002 because Entities will need to re-evaluate their CIP-002 what is IN vs OUT. For example, some ROM devices may fall under CIP-002. This subtle change may force a new version of CIP-002 assessment - the new definition would bring in more devices that would not be considered programmable and the changes would not be backward compatible.

New definition will bring in more devices (ROM, firmware, etc.) that are typically not considered programmable

Since the Standard should be technically agnostic, we recommend not calling out virtual hardware (virtualization).

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

MEC does not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the "how to comply" with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

MEC believes that the SDT should retain the defined terms “BES Cyber Assets (BCA)” and BES Cyber System (BCS) as currently written. We also believe that given the proposed revisions made to the term “Cyber Asset”, which clarify that physical or virtual hardware, software and data are allowed, obviates the need to revise the other definitions.

Likes 0	
Dislikes 0	

Response
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer	No
Document Name	

Comment

Dominion Energy has comments on the following proposed definitions:

- PAMS – It is unclear if the intent is to collect visitor logs (paper or substation voice system).
- LIZ – 1) It is unclear if an entity has multiple VLANs behind the firewall that the entity could claim it’s in a single ESP under the proposed definition. In addition, it is unclear if an entity can mix logical isolation zones in virtual environments on a single piece of hardware. Additional clarity should be added around which entity actually defines the LIZ (either the ERO or the Entity). Finally, it is unclear on whether the communication links mentioned in 4.2.3.3apply only if the ERO determines it extends one or more geographic locations.
- IRA – Additional clarity needs to be added on what “remote access client” means. It could be interperted to be either protocol or client.
- RM – Please clarify the first bullet. Would this apply to flash drives that are smart/have chips in them? We recommend adding the examples back for clarity.

Likes 0	
Dislikes 0	

Response
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS does not agree with the proposed change in the BCS definition, unless the new Cyber Asset term is added to the definition of BCS to maintain the reference to/inclusion of the term “programmable.” Specifically, the revisions to BCS do not adequately describe the Cyber Assets that would comprise a BCS without the use of the word “programmable” because the fact that a Cyber Asset is “programmable” sets the foundational criteria by which assets and/or BCS are considered for CIP categorization. Without a reference to the term “programmable,” an inconsistency between the term Cyber Assets and BCS is introduced as is the potential that the scope of assets to be considered under the BCS classification will be unclear. To ensure consistency and reduce the potential for confusion, AZPS requests that the term “programmable” be included in the new BCS – either directly or indirectly through replacement of “hardware (including virtual hardware), software (including application virtualization), and data” with “Cyber Assets”.

Further, AZPS notes that the Standards Authorization Request form for this Project (“the SAR”) outlined that the SDT would be responding to the V5TAG Transfer Document request for clarification of “the intent of ‘programmable’ in Cyber Asset, and a focus on the definition of ‘BES Cyber Asset’ so that it does not subsume all other cyber asset types.” AZPS notes that this draft does not provide the necessary clarity regarding the intent of “programmable” and may go beyond the scope of the SAR by retiring the term BES Cyber Asset and fundamentally changing definitions and the requirements in which they are utilized across all CIP Standards.

For these reasons, AZPS requests the rationale for how the retirement of the term BES Cyber Asset and the modifications to BCS meet the intent of the SAR as well as clarification on the reasoning (generally) behind the retirement of the term BES Cyber Asset and the removal of references to “programmable” that results from the proposed revisions to the two foundational definitions associated with the CIP reliability standards (BES Cyber Asset and BCS). As discussed above, AZPS suggests additional revisions to recapture the term “programmable.” An alternative approach could be to develop a new definition and/or classification for virtualized assets, which definition/classification would then be added to the applicability tables, as appropriate.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry’s programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

The new definition expands the scope of devices that would fall into CIP regulation if the Cyber Asset term is removed by removing the BCA component. Currently only programmable electronic devices are in scope. The new definition would bring into scope electronic devices that are not capable of being updated; no means to update the software or firmware within them (not field updateable). These devices currently do not meet the “programmable” electronic device definition and are thus out of scope for NERC CIP.

We recommend leaving the BES Cyber Asset and, BES Cyber Systems definitions and accepting the proposed Cyber Asset definition. We feel this allows for virtualization and significantly reduces the documentation changes that would be required by the elimination of the BCA definition

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No

Document Name	
Comment	
The new BCS definition exludes the use of the term “Cyber Asset”. “Cyber Asset” was also redefined and used in other defined terms such as TCA’s, etc. To be consistent, we suggest the following definition for BCS “A single or combination of Cyber Assets, regardless of redundancy, performing one or more….” Since the new definition of Cyber Asset is inclusive of the hardware (physical or virtual), software and data in the devices, it makes sense to utilize the term consistently in other new/revised definitions since not all devices lend themselves to be “systems”. (i.e. stand-alone assets or components of a system).	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
By excluding the term programmable from the proposed BCS definition, the SDT risks bringing into scope devices that were previously excluded from BCSs due to not being programmable. In the guidelines and technical basis of CIP-007-6, an unmanaged switch is listed as an example of a nonprogrammable device. As a nonprogrammable device, an unmanaged switch did not meet the definition of a Cyber Asset and therefore could not meet the definition of a BES Cyber Asset. Under the proposed BCS definition, an unmanaged switch meets the BCS definition. An unmanaged switch is hardware, it contains software (the firmware the switch is running), and it contains data (the MAC address table). If this proposed change is implemented in its current form then entities may need to re-evaluate the criteria used to determine what devices should be included in BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP does not agree that the BCS definition describes the BCS appropriately. The new definition is attempting to combine many definitions into one. SRP suggests using the language below:	

A BES Cyber System includes any combination of programmable hardware (including virtual hardware), software (including application virtualization), and data, regardless of redundancy, where:

1. It/they performs one or more reliability tasks; and
2. If rendered unavailable, degraded, or misused, the situation would result in adverse impact to one or more BES Facilities within 15 minutes.

Additionally, the term ”programmable” should remain in the definition of a BES Cyber System. “Programmable” excludes certain IT network components such as patch panels, patch cables, etc. which should not be in scope.

SRP also agrees with APPA’s comments.

Likes 0	
Dislikes 0	

Response

Jamie Prater - Entergy - 5,6

Answer	No
Document Name	

Comment

The removal of the BCA term and failure to include programmable in BCS can potentially expand the scope of applicable devices to an entity.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Support MRO NSRF Comments

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy requests further clarification on the proposal for BCS definition. The proposed definition indicates that there should be a “combination of hardware, software, and data”. Is it the drafting team’s intent there must be a combination of any of those elements (hardware, software, data), or can something be considered as a BCS if it contains only one of those elements (software)? Without the use of the term “programmable” can an entity infer that an asset that is hardware only, not be considered a BCS?	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
WAPA does not support retiring the term BES Cyber Asset. WAPA recommends the term BES Cyber Asset be retained and used as it is currently defined in all applicable definitions in the NERC Glossary of Terms. WAPA also does not support the proposed definition of BES Cyber System. Defining BES Cyber System without using the term “BES Cyber Asset” (to include the term “programmable”) could bring equipment like PTs, CTs, pressure sensors, temperature sensors, and other hardware devices for BES functionality into scope.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company is concerned that ultimately, this will depend on the audit methodology. If the objective of the requirement is measured to see if it is met on the BCS as a whole, then this should work. If the objective is measured on every physical device in the system, then it will fail. The term "Programmable" may still be needed as a scoping mechanism if the audit approach does not change to match the system approach.	

Southern Company is also concerned that in using the phrase “adverse impact to one or more BES Facilities”, auditors may interpret this as a considerable expansion of the scope of what is encompassed by the definition.

We understand that the F in Facility has been capitalized by the SDT intentionally and in this definition, means:

“A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)”

Therefore, it appears to Southern that this is **not** intended by the SDT to expand the scope of what is currently included, out to systems such as Fire Protection Systems, HVAC and other systems which do not have a direct impact upon the BES. Southern Company also believes that the way in which it is written will not change the scope of the Standard in respects to the inclusion of Control Centers and their associated Data Centers. As noted in CIP-002-5.1a,

“Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.”

As long as the intent behind the quote above from CIP-002 does not change in future revisions, Southern feels the intent remains the same with the proposed wording of the definition of Cyber Asset as it relates to “BES Facilities”.

Southern Company is concerned that unless the SDT finds a way to ensure that the current scope remains unchanged, our Operations groups will suffer an undue compliance burden, spending an inordinate amount of time providing evidence of minutiae while likely seeing little of the direct benefits of virtualization.

That said, Southern Company would like to see additional clarity provided in future revisions of this proposed change regarding maintaining the scope of the Standards to what is *currently* in scope. This will allow us to balance implementing the benefits of virtualization while also providing reasonable proof demonstrating a secure implementation.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group

Answer	No
Document Name	

Comment

Because the concept of “programmable” is retained in the defined term “Cyber Asset” (which is an element of a BES Cyber System), industry needs guidance on what constitutes a “programmable” electronic device. Additionally, the new definition for BES Cyber System includes electronic devices that are not capable of being updated (i.e, no means to update the software or firmware within them (not field updateable)). Therefore, because these devices currently do not meet the “programmable” electronic device definition, such devices should be out of scope for NERC CIP.

Finally, for consistency with the revised definition of Cyber Asset, the definition of BES Cyber System should read: “Any combination of physical or virtual hardware (including virtual hardware), software…”

Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA	
Answer	No
Document Name	
Comment	

We recommend returning the “programmable” language to the BCS definition, as well as maintaining a definition of BES Cyber Asset as a component of the BCS. We believe these changes improve backward compatibility.

This proposed change ripples into CIP-002 because Entities will need to re-evaluate their CIP-002 what is IN vs OUT. For example, some ROM devices may fall under CIP-002. This subtle change may force a new version of CIP-002 assessment - the new definition would bring in more devices that would not be considered programmable and the changes would not be backward compatible.

New definition will bring in more devices (ROM, firmware, etc.) that are typically not considered programmable

Since the Standard should be technically agnostic, we recommend not calling out virtual hardware (virtualization).

Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

The current definition of a BES Cyber System only includes programmable electronic devices. The proposed definition would draw in non-programmable devices. Currently non-programmable device are not in scope for CIP Compliance and should not be included since there are no means to update non-programmable devices. We recommend keeping the current definitions for BES Cyber Asset and BES Cyber System.

Likes 0	
Dislikes 0	

Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Tri-State would like clarification on how the new definition of BES Cyber Systems (BCS) will be used to evaluate Low Impact BCS. Previously the BES Cyber Asset definition could be utilized to eliminate programmable devices from being included within the Low Impact BCS. How would the new definition allow for the removal of programmable devices that while connected to a BCS, could not effect it within 15 minutes?	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BHC is concerned that the BCS proposed definition does not highlight "cyber" assets, therefore a transformer or electro-mechanical relays could be considerd part of a BCS. Additionally, the term "and data" should be removed from the BCS Cyber System definition as it is too ambiguous. BHC proposes the following definition: One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST. In addition, we ask the SDT to consider a review of CIP-002 along with the definitions of Cyber Asset, BES Cyber Asset, and BES Cyber System. The SDT's approach to address applicability of cyber security controls to the virtualized	

functions will result in significant amount of work to make the existing documents (plans, processes and work instructions) conform to the new definitions and the risk based approach.

Likes 0	
Dislikes 0	

Response
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment
EEI members who participated in the development of these comments do not support the changes made to the term BES Cyber System (BCS) or the retirement of BES Cyber Asset (BCA). However, we understand that other members are more supportive of the changes. As a result, these comments do not represent a consensus, but we offer them for the SDT to consider. EEI understands the SDT's desire to move from the current asset focused model to a systems approach, but the changes being proposed within the body of revised and retired definitions appears to go well beyond the EEI members' understanding of the scope and intention of the currently approved SAR. EEI recommends that the SDT retain the defined terms "BES Cyber Assets (BCA)" and BES Cyber System (BCS) as currently written. Further, EEI observes that the proposed revisions made to the term "Cyber Asset," which clarify that physical or virtual hardware, software and data are allowed, obviate the need to retain the other definitions.

Likes 0	
Dislikes 0	

Response
David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

The proposed definition of BCS does not address the issues and interpretations that surfaced by not having a definition of "programmable."

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

NRG asserts that the proposed definition of BCS would include the SCADA traffic itself (not just the data that exists within the hardware). Therefore, change control would need to include source control. This could be a challenge for the industry. NRG recommends that NERC SDT work to include definition delineation and classification delineation of data at rest versus data while in transit as critical relating to the definition of Cyber Asset and BES Cyber System. Expanding the definition beyond data on devices, could cause entities to have to re-define BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

The proposed definition does not address the issues and interpretations that have been raised by not having a definition of programmable. Furthermore, the definition uses the phrase “Any combination of hardware (including virtual hardware), software (including application virtualization), and data.” The term “combination” does not mean a combination including at least one of each. Instead, a combination could have a null element in a set. For instance, you could have a combination of only hardware, no software, and no data as a valid combination set. So, if you look at the definition with that in mind you could have hardware “performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.” This could easily be a breaker or some other item in a station that is made of only hardware. This has now opened a Pandora’s box of compliance issues and need for clarification rather than help resolve anything.

We would propose that the definition say something like, "Any combination of Cyber Assets, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes." We would also prefer the term "programmable" in the definition of Cyber Asset be further clarified.	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Programmability is a fundamental concept that sets the scope of applicability for the current CIP standards. While many standards will not apply, there are a number of requirements that aren't obviously tied to the ability of a device to be programmed. Including non-programmable hardware fundamentally changes the landscape of the CIP standards (i.e. breakers and motor-operated switches could now be in scope). Simply inserting "programmable" in front of the first instance of "hardware" in the definition would at least give the same scope as we have today (although the term "programmable" would still be fundamentally undefined and subject to individual interpretation).	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Cowlitz agrees with comments submitted by APPA. We agree with the intent of the SDT, but are concerned with the lack of clear identification/scoping towards computer systems.	
Likes 0	
Dislikes 0	
Response	

2. The SDT asserts that the proposed Cyber Asset definition provides clarity around virtual hardware. (Cyber Assets revised definition: Programmable electronic devices, including the physical or virtual hardware, software, and data in those devices.) Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
See proposed Cyber Asset definition above. We believe the proposed definition is more appropriate and achieves the intended objective.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy does not object to the clarifying changes made to the term Cyber Asset (i.e., they can be physical or virtual); however, we do not believe the change was necessary because virtualization is currently allowed under the current CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Exelon does not object to the clarifying changes made to the term Cyber Asset (i.e., they can be physical or virtual); however, we do not believe the change is necessary because the use of virtualization is not prohibited under the current CIP Standards.	
Likes 0	
Dislikes 0	

Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	Yes
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "EEI does not object to the clarifying changes made to the term Cyber Asset (i.e., they can be physical or virtual); however, we do not believe the change was necessary because virtualization is currently allowed under the current CIP Standards."	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy requests further clarification on the use of the phrase “virtual hardware”. For example, if an entity sets up a virtual switch in the “virtual hardware”, would this be considered a separate asset? Futher examples of what the drafting team considers “virtual hardware” would be beneficial to the industry.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the definition. However SRP requests further clarification and guidance on this term as this definition will increase the scope of applicable Cyber Assets.	
Likes 0	

Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
See response to Question 1 above.	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Agree. Assume the intent of the proposed definition is to include all instances of a device, even when multiple instances exist simultaneously. Virtual hardware = a logical instance of a device of which multiple versions could exist simultaneously	

Physical hardware = the physical instance of a device of which only one version can exist at a time	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
The word hardware is confusing since a hardware can't be really "virtual". We propose to use the word "virtual ware" or "virtual machine".	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes
Document Name	
Comment	
MEC does not object to the clarifying changes made to the term Cyber Asset (i.e., they can be physical or virtual). However, we do not believe the change was necessary since we believe virtualization was not forbidden within the current body of CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Note, the proposed Cyber Asset definition included in the question is not the same as that included in Table 1 of *2016-02_CIP_Definitions_Redline_11022018.pdf*, 'A programmable electronic device, including the physical or virtual hardware, software, and data in the device.' These two definitions should be aligned.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	Yes
Document Name	
Comment	
Cowlitz agrees with the SDT. However, consideration of the comments provided by APPA is cause for concern. The new language should not require revision of compliance efforts for non-virtual application. Cowlitz believes dual treatment as suggested by APPA is one possible solution, but placed in the definition of BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

EEI members who participated in the development of these comments do not object to the clarifying changes made to the term Cyber Asset (i.e., they can be physical or virtual); however, they do not believe the change was necessary because virtualization is already permissible under the current CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with this change.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	

The Cyber Asset definition included in the question should mirror that which was included in Table 1 of 2016-02_CIP_Definitions_Redline_11022018.pdf, ‘A programmable electronic device, including the physical or virtual hardware, software, and data in the device.’	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
Public power is concerned that the new definition will require new evidence and will not work with the existing approach structured around the CIP Evidence Request Spreadsheet (v2.0). Public power is also concerned that the list of BES Cyber Assets used for sampling will no longer be feasible, therefore it is not clear what approach auditors may require. In addition, documentation of the virtual host and virtual guests will only be a snapshot in time making it difficult to demonstrate compliance for individual cyber asset level security controls. APPA believes it would be clearer to maintain the BCA definition for physical devices, while providing new definitions for virtual devices (Virtual Cyber Asset), or consider a dual-definition approach (see response to Question 3).	
Likes 0	
Dislikes 0	

Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Adding “virtual” to the definition does not affect the clarity of the definition, it only includes a new subsect of devices. It may be more prudent to create a separate term and definition for Virtual Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO recommends that the SDT define “programmable” or provide guidelines regarding the difference between a non-programmable electronic device and a programmable electronic device.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
The proposed definition of cyber asset just adds the words “or virtual” to the definition, but continues to leave known issues with the current definition unaddressed. Most of these issues are related to the use of the term programmable. It is recommended that the team further evaluate the definition and consider migrating from the term programmable to a less ambiguous term. While “programmable” or a suitable variation of the term is needed, the issues with the current non-definition of programmable need to be addressed. The definition is based on programmable, the various types of programmability needs to be addressed: (1) Remotely programmable; (2)	

requires physical access and interruption of operation to change device programming; Electromechanical devices (including devices such as electromechanicable breakers and physical hardware such as communications cabling and electrical wiring)	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 2.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	

Please clarify the following; (1) programmable needs to be defined to provide clarity between devices that are truly programmable via logic and those that require component changes to update, (2) the meaning of application virtualization, specifically in regards to containerization, and (3) how entities are expected to inventory discreet devices to show relationship to the BCS.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC agrees with the wording recommended by AZPS. “A programmable electronic device, including hardware, software, and data in those devices, ***whether physical or virtual***.”	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	AZPS Comments - Question 2.docx
Comment	

Please see the attached document.

Likes 0

Dislikes 0

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion

Answer No

Document Name

Comment

Likes 0

Dislikes 0

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer No

Document Name

Comment

Since the Standard should be technically agnostic, we recommend not calling out virtual hardware (virtualization) and do not call out physical. IOW, keep the existing Cyber Asset definition.

Likes 0

Dislikes 0

Response

Joseph Pride - Trans Bay Cable LLC - 1 - WECC

Answer No

Document Name

Comment

The definition only helps address virtualization to the level of discrete virtual machines. It does not adequately cover more advanced edge cases that blur the lines between virtual machines. Examples of edge cases could include collections of machines like supercomputing clusters that share resources such as memory, or (more commonly) network storage. Examples could also use containerized assets, which may share a substantial amount of the OS and software without duplication, running specific software within walled containers.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

The virtual hardware is vague and causes confusion. We suggest using the previous revised Cyber Asset definition as follows:

"A programmable electronic physical or virtual device, including the hardware, software, and data in the device. Each virtual machine and host is a distinct device." Given that the virtual device can be captured separately using this previously proposed definition, additional requirements that may be developed only apply to the virtual devices if the current requirements don't fit them.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Response should be "YES". The program doesn't allow editing of the button.

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

This definition works to capture virtual hardware.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
While the revision provides some clarity around virtual hardware, “programmable” remains a debated topic that should have more clarity regarding what is programmable and what isn’t because component changes are required. The definition does not address application virtualization which is another virtualization technology that can be employed. In relation to the BCS comment, Cyber Asset needs to remain a component of BCS because otherwise how does an entity define what the composition of the System is?	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Please clarify the following: (1) programmable needs to be defined to provide clarity between devices that are truly programmable via logic and those that require component changes to update; (2) the meaning of application virtualization, specifically in regards to containerization; and (3) how entities are expected to inventory discreet devices to show relationship to the BCS.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST. In addition, we recommend that the SDT focus on functionality in defining Cyber Assets (e.g. information technology and electronic components that systematically receive inputs and produce desired outputs) rather than whether it is virtual vs. physical or programmable vs. non-programable.	

Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
We believe it would be clear to keep the current BES Cyber Asset definition for physical devices and provide new stand alone definitions for virtual devices.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA	
Answer	No
Document Name	
Comment	
Since the Standard should be technically agnostic, we recommend not calling out virtual hardware (virtualization) and do not call out physical. IOW, keep the existing Cyber Asset definition.	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	No
Document Name	
Comment	
What is “virtual hardware”? The SSRG recommends the SDT define virtual hardware to ensure consistent application across industry and in audit situations. Likewise, due to the programmable aspect of a Cyber Asset, “virtual” software is delivered by a vendor (rather than coded by the responsible entity) and, therefore, is not a physical programmable device (ie., hardware). Given this, how does programmable apply to virtualization software?	

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

Comments: MRO supports the intent to accommodate virtualization within the NERC Glossary terminology, but the term “device” is generally understood to be a hardware specific physical term and cannot be grammatically supported to also represent something that is virtual as has been attempted in the proposed redefinition of Cyber Asset. This grammatical conflict may yield to extensive interpretation which may hamper consistent CMEP implementation by the ERO. One option for incorporating virtual components into the Cyber Asset term could be to add a layer beneath the Cyber Asset term so that the programmable electronic devices language can remain (representing physical hardware devices), and a new defined peer term like “Virtual Programmable Asset (VPA)” or “Cyber Element” could be added to identify VPAs that have no physical form. We recommend consideration of the following terms (organized like a schema - includes hierarchy), which permit the incorporation of VPAs while insulating impact to existing NERC CIP glossary terms:

- PED (programmable electronic device) – this can remain undefined, but we understand it to be hardware based. A device is a physical thing and can’t be virtual itself but can host other Virtual Programmable Assets
- Virtual Programmable Asset (VPA – more basic than a Cyber Asset): Includes software and data, but does not include physical hardware
  - Cyber Asset: PEDs and VPAs, including hardware, software, and associated data
    - BES Cyber Asset – (remains as defined)
    - BES Cyber System – (remains as defined)
    - PCA (Protected Cyber Asset) – (remains as defined)
    - EACMS – (remains as defined)
    - PACS – (remains as defined)

Likes 0	
Dislikes 0	

Response

3. The SDT asserts that the term Cyber Asset should continue to be used within the NERC Glossary of Terms for: Removable Media and Transient Cyber Asset. Due to the nature of that type of hardware, these devices do not lend themselves to the systems approach. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	Yes
Document Name	

Comment

SMEC agrees that the term Cyber Asset should remain in the Glossary of Terms, but does not believe it should be limited to Removeable Media and Transient Cyber Asset.

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	Yes
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	Yes
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"EEI agrees that the term Cyber Asset should remain in the Glossary of Terms but does not believe it should be limited to Removeable Media and Transient Cyber Assets. The term should continue to be used throughout the CIP standards utilized in its current form."

Likes 0	

Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Exelon agrees that the term Cyber Asset should remain in the Glossary of Terms but does not believe it should be limited to Removeable Media and Transient Cyber Assets. The term should continue to be used throughout the CIP standards utilized in its current form or as proposed to be revised.

Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

CHPD agrees that the term Cyber Asset should continue to be used within the NERC Glossary of Terms for: Removable Media and Transient Cyber Asset.

Additionally, consider how this same issue applies to traditional non-virtual hardware-based BES Cyber Assets. If an exception is being granted for specific existing hardware device types, then perhaps the problem should be flipped to instead consider the virtual systems to be the exception to the rule. Using this thinking, it may make more sense to instead develop separate virtualization language that is then referenced in the existing Cyber Asset and BES Cyber System definition. This would enable the language to expand scope to allow virtual environments without throwing out the existing scoping language for existing non-virtual Cyber Assets.

This could be accomplished with something like the following:

Virtual Cyber Asset (VCA) – Programmable virtual system that is comprised of a virtual operating system and the host hardware and software that hosts the virtual operating system.

BES Cyber System (BCS) - A combination of one or more Cyber Assets or Virtual Cyber Assets performing one or more reliability tasks, including redundant members that support a reliability task, that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.

Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
NV Energy agrees that the term Cyber Asset should remain in the Glossary of Terms, but does not believe it should be limited to Removeable Media and Transient Cyber Assets. The term should continue to be used throughout the CIP standards utilized in its current form.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The NSRF agrees that the term Cyber Asset should continue to be used within the NERC Glossary Terms for: Removable Media and Transient Cyber Asset. The NSRF does not agree with making other changes to the Removable Media and Transient Cyber Asset definitions. Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	

We still support the current device-centric requirements for both physical and virtual devices as we are doing today rather than only for the TCA/RM. The device-centric approaches are more manageable and auditable.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	Yes
Document Name	

Comment

Reclamation agrees that Removable Media and Transient Cyber Assets are not BES Cyber Systems. Reclamation recommends the continued use of the term Cyber Asset, not just for Removable Media and Transient Cyber Asset, but for all applicable definitions in the NERC Glossary of Terms.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	Yes
Document Name	

Comment

We agree that the term Cyber Asset should remain in the Glossary of Terms but do not believe it should be limited to Removeable Media and Transient Cyber Assets. The term should continue to be used throughout the CIP standards utilized in its current form.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	Yes
Document Name	

Comment

MEC agrees that the term Cyber Asset should remain in the Glossary of Terms but do not believe it should be limited to Removeable Media and Transient Cyber Asset. Rather, we believe that the term should continue throughout the CIP standards utilized in its current form. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the "how to comply" with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

Agree

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

Although AZPS agrees that Removable Media and Transient Cyber Assets should remain at the Cyber Asset level, this is only consistent if the changes to the definitions and/or associated approach to classification/applicability recommended in our response to Question No. 1 are incorporated.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
: See response to Question 1 above.	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Support MRO NSRF Comments	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	Yes
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern believes the retirement of the term BES Cyber Asset accomplishes the purpose and the generic Cyber Asset is still appropriate for those areas in the standard where a device level is appropriate, such as TCAs. Due to the nature in which they are used, Transient Cyber Assets should continue to be viewed as individual assets that can be grouped for compliance and reporting reasons. The proposed changes reflect this.

Likes 0	
Dislikes 0	

Response
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment
EEI agrees that the term Cyber Asset should remain in the Glossary of Terms but our members who participated in the development of these comments do not agree that it should be limited to Removable Media and Transient Cyber Assets. The term should continue to be used throughout the CIP standards in its current form with its current scope and applicability.

Likes 0	
Dislikes 0	

Response
Gladys DeLaO - CPS Energy - 1,3,5

Answer	Yes
Document Name	

Comment
Agree that TCAs should still be kept at the Cyber Asset level.

Likes 0	
Dislikes 0	

Response
David Jendras - Ameren - Ameren Services - 1,3,6

Answer	Yes
Document Name	

Comment

Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Agree that TCAs should still be kept at the Cyber Asset level.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
In relation to the BCS comment, Cyber Asset needs to remain a component of BCS because otherwise how does an entity define what the composition of the System is?	

Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0

Dislikes 0

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	
Document Name	

Comment

Seattle City Light contributed to and supports the comments provided by APPA.

Likes 0

Dislikes 0

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment

No comment.

Likes 0

Dislikes 0

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE suggests the term Cyber Asset should continue to be used in defining all system definitions, such as Removable Media, Transient Cyber Assets, and BES Cyber System. A system is one to many Cyber Assets, regardless of whether the Cyber Asset is physical or virtual. Removing the term Cyber Asset from the system definition loses the hierarchy that is in place.

Texas RE is concerned there will be a gap because not every cyber asset in the system will be protected under the new definition. Treating the virtual machine and its host as separate Cyber Assets may result in mixed-trust virtual environments, which exacerbates vulnerabilities as the host runs CIP and corporate virtual machines. CIP controls are only being applied to the CIP virtual machine and not its host; even though the host "if rendered unavailable, degraded, or misused" can affect the CIP and corporate virtual machines. In addition to certain assets not being protected, Texas RE is concerned these changes could lead to an increased effort for entities to provide evidence of their identification of BES Cyber Systems and for Regional Entities to audit.

If the SDT elects to eliminate the term Cyber Asset, Texas RE recommends the following BES Cyber System (BCS) definition:

One or more Cyber Assets, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.

Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	

APPA believes the SDT should consider the concept of two (parallel) definitions, at least for a time, and a sort of "virtualization overlay" for the CIP Standards. Instead of replacing the definitions and Standards, create options whereby an entity can select, for any particular cyber system, to use the existing V5-6 definitions and Standards, or new virtualization definitions and Standards. It is up to the entity to make clear in advance which approach they choose for each cyber system.

As a practical matter, it is anticipated that there would be a single Standard in each case, but that it would include all the existing Parts as well as all the new proposed Parts (as modified by comments) to accommodate virtualization, with language directing an entity to select, for each cyber system, which of the two sets they will adhere to.

In this way the extensive changes to allow virtualization can be piloted by those entities most involved, while other entities can continue their CIP practices as at present, which accommodates the backwards compatibility concept. Over time, industry can learn whether the changes represent a real advance or introduce a large number of unintended consequences, and work to improve the Standards.

As such, all existing definitions would be retained in parallel to the new ones proposed in this effort.

This concept might be considered somewhat analogous to that used for the transition from PRC-005-2 to PRC-005-6, modified for use in virtualized and non-virtualized environments.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

Cyber Assets are still discrete parts of a BCS either physical or virtual and must remain a term across the standards. Limiting the use of Cyber Asset to TCA and RM becomes problematic when looking at the way a Cyber Asset that is included in a BCS is disposed of as a part of CIP-011 R2.1 and R2.2. Either the language in CIP-011 must be changed or this question needs to be rewritten to clarify the impacts to CIP-011 as well.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 3.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
The "systems" approach is flexible and has value when used for any CIP Cyber Assets. The "system" grouping can be applied arbitrarily and applicability only relies on an entities approach. In one context, the use of "Cyber Asset" versus "Cyber System" is valuable to be able to distinguish a single "device" that is included in a Cyber System. The entity just needs to be diligent in how they define their "Cyber Assets" and "Cyber Systems" to ensure they effectively provide value. We agree that Removable Media does not lend itself well to the "systems" approach. Unlike a Transient Cyber Asset (example, a laptop) that includes a combination of hardware, software, data, etc., the typical Removable Media is only media used for transferring and/or storing code and/or data.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. No changes to proposed Removable Media. PAC is suggesting some minor adjustments to the TCA definition:	

Transient Cyber Asset - A Cyber Asset that is: 1) capable of transmitting or transferring executable code, 2) not included in a BES Cyber System, 3) not [included in] a Protected Cyber System (PCS) associated with high or medium impact BES Cyber Systems, and 4) directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: 1) BES Cyber System (BCS), 2) network within a BES Cyber System Logical Isolation Zone containing high or medium impact BES Cyber Systems, or 3) PCS associated with high or medium impact BES Cyber Systems. [delete the remaining examples text] Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes that a more effective approach would roll up the requirements that currently depend upon that term for applicability and retire the term Cyber Asset itself. Security controls for removable media can easily be a subset of controls applied to any transient device. Rather than a defined term "Cyber Asset" which then has "Transient" pre-pended, either TCA (including removable media) can be a defined term with requirements applied to it, or the requirement can simply apply to transient devices with no special term required.	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	No
Document Name	
Comment	
Transient Cyber Assets could be better considered as Transient Cyber Systems. There may be virtualized systems that blur the line between individual or multiple assets. It may be possible to “virtually” change a Transient Cyber System’s location from inside the Logical Isolation Zone to outside, allowing it to transit. Depending on how virtualization is implemented, it may make sense to manage multiple or blurred assets on a Transient Cyber System level. The key elements of a Transient Cyber System are that the entire system is either inside the LIZ (for 30 days or less) or outside at any one time, but never both at the same time. Operating by this definition would still make asset-level management appropriate where discrete Cyber Assets such as laptops are used.	
Likes 0	
Dislikes 0	

Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Has the drafting team considered modifying the terms Removable Media and Transient Cyber Asset rather than keeping the Cyber Asset definition? This may be a better approach long term, rather than keeping a term around to clarify other existing terms.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The term Cyber Asset is also used in the revised definition of ERC. We recommend keeping the current definitions for BES Cyber Asset and BES Cyber System.	
Likes 0	
Dislikes 0	
Response	

4. The SDT is proposing to retire EACMS and develop two new terms: EACS and EAMS. These terms will allow changes within the applicability for the monitoring portion to allow third party monitoring systems. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
We agree that the seperation allows for the utilization of a third party. We have concerns regarding the security controls that will no longer apply to the monitoring systems. This is especially concerning when considering the aggressive timeframes for response to detected conditions.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
We appreciate the SDT clarifying the differences between access control and access monitoring and support the new definitions. We request additional details regarding the reduced applicability of the EAMS.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
We appreciate the SDT clarifying the differences between access control and access monitoring and support the new definitions. We request additional details regarding the reduced applicability of the EAMS.	
Likes 0	

Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	Yes
Document Name	

Comment

Please clarify how an entity would classify and asset that performs and EACS and EAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify is EAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if EAMS is to be treated similar to BCSI, which appears to be the case.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	Yes
Document Name	

Comment

SMEC agrees with the separation of EACS and EAMS, but there needs to be more guidance provided including how to document cases when they are implemented as the same, or with overlap.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP agrees. This will help to prioritize the protection of Electronic Access Control Systems.

Likes 0	

Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that developing two terms for EACS and EAMS is appropriate.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We conceptually agree with the concept of splitting EACMS into EACS and EAMS. Some guidance should show clearly that EACS can be used for backwards compatibility purposes with current EACMS devices.	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	
Comment	
These are indeed two separate classes of System (although in some cases they can be implemented as the same, or with overlap). The split will only be meaningful as it can be used to separate which Requirements are applicable to each.	
Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	Yes
Document Name	

Comment

We agree to separate the EACS and EAMS from EACMS. The EAMS may be treated as a BCSI repository that is allowable to be managed by the third party as long as there is a NDA in place.

Likes 0

Dislikes 0

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

BPA suggests adding the following clarification to this question regarding security requirements for EAMS: “Under the proposed new definition EAMS can safely exist outside of a Logical Isolation Zone, under a reduced set of applicable requirements that allow entities to use additional methods to monitor and correlate access log entries.” This may require modification to CIP-004 R4.2 to allow the entity to accept verification of electronic access authorization for third parties other than at the individual level, perhaps based upon contract statements of work (SOW) or service level agreements (SLA).”

Likes 0

Dislikes 0

Response

Leanna Lamatrice - AEP - 3,5

Answer	Yes
Document Name	

Comment

More guidance is needed to apply these new definitions to management systems like patching management, SIEMs, Anti-Virus, vCenter. Should these systems be consider EACS or EAMS?

Likes 0

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Using these services, third parties will still fall under the CIP-004-7 PRA requirements and access control of BCSI in CIP-011-2.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Button respons should be "No". Editing of the button isn't possible. PacifiCorp’s approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. PAC believes that this can still be accomplished by maintaining the EACMS term and altering the existing definition. It will allow entities the flexibility to define the different devices that are EACMS and what duties they perform. Third party monitoring still fits into the scope of the original definition of EACMS. Based on the current proposal of EAMS and EACS, systems like SEIM and IDS would be categorized as EAMS. EAMS does not show up in any of the current draft versions of the Standards, it is unclear if this was the SDT’s intent. Proposed change to existing definition for EACMS: **EACMS** - Cyber Assets or [systems] that [delete – perform] [provide] electronic access control or electronic access monitoring of [delete - the Electronic Security Perimeter(s) or] BES Cyber Systems. This includes Intermediate Systems.	
Likes 0	
Dislikes 0	
Response	

James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
I do not foresee a big impact for CPS Energy with the split of EACMS in two.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Please clarify how an entity would classify an asset that performs EACS and EAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify whether EAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if EAMS is to be treated similar to BCSI, which appears to be the case.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
We suggest adding the following clarification to this question regarding security requirements for EAMS: "Under the proposed new definition EAMS can safely exist outside of a Logical Isolation Zone, under a reduced set of applicable requirements that allow entities to use additional methods to monitor and correlate access log entries."	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company believes that this change is one that will allow for more granular scoping and grouping of systems so that protections can be consistently applied at appropriate levels. Along with the proposed term PAMS, the additional flexibility that this change will provide opens up the possibility to use security and analysis services that cannot currently be used while preserving backward compatibility.

Southern agrees with this direction and believes it will greatly help with the sharing of logging information for detection of cyber-attacks and indicators of compromise. It is a big step towards allowing correlation of events with non-CIP network activity and the sharing of information with entities or agencies that may have classified intel for use in the analysis of log data. Southern requests that as the SDT considers this area and its relationship to BCSI, that the SDT consider the implications to “off premise repositories” of this log information that is shared with external parties for further analysis. Southern believes the risks of this should be covered contractually with NDA's for example, and not covered by system level requirements on the off-premise systems on which this data resides. With that in mind, Southern suggests the SDT consider the need for EAMS and PAMS definitions.

Also, while CIP-011-2 was not included in this round of informal comments, the scope within CIP-011-2 will need to be refined to accommodate the new terms but we understand that this further refinement is planned.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	
Comment	

Cowlitz supports APPA comment.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	
abstain	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
With respect to the proposed EAMS definition, what is meant by “Cyber systems that provide electronic access monitoring”? Is the term intended to refer to systems that are monitoring the “electronic access”? Or does the term mean that EAMS are performing electronic monitoring of the BCS (such as Tripwire, patch management solutions, SIEM tools, etc.)? The EACS definition is clear that a device/system is controlling electronic access to the BCS. Guidance on EAMS should include what systems are anticipated to be considered EAMS. Currently, EAMS are only applicable under CIP-004. In the event of a third-party service monitoring EAMS and PAMS, it may be extremely difficult to authorize access and revoke access in a timely fashion for individual employees at said third-party service. This requirement will need further compliance guidance. As written now, the Standard introduces for EAMS and PAMS the same unresolved challenge as exists the use of third-party cloud providers for BCS storage. The EACMS vs. EAC/EAM definition discussion presents the same possibility for two parallel definitions as discussed above in response to Question 3. Why not retain the EACMS definition and introduce the new option for EAC/EAM definitions as well? Entities must state which definition they use for each applicable cyber system. There is no security necessity at this time to force all to change to accommodate virtualization, when only some entities are pursuing such approaches. Both options are feasible at present.	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE does not agree that separating EACMS into two separate terms is necessary. It appears that separating EACMS into EACS and EAMS and updating the applicability of various requirements based on this new distinction is acting to remove the applicability of some requirements, including security, from purely monitoring systems. This would decrease cyber security and the defense in depth posture. Based on the changes in the applicability to EAMS that were proposed, such as CIP-004-7 R3 regarding PRAs, it appears as though we would be allowing for third party monitoring by removing requirements that are difficult for entities to impose on third parties.

In regards to the language of the proposed ECMS and EAMS definitions, the SDT uses “cyber system”. This is not consistent with the language used in the proposed BES Cyber System definition. Entities also use virtualization for their EACMS. Texas RE proposes that the EACMS definition also use the Cyber Asset term, and the Cyber Asset term will allow for virtualization.

Rather than breaking EACMS into two terms, Texas RE recommends the following revised EACMS definition:

Cyber Assets that perform authentication, monitoring and logging, access control, interactive remote access, or alerting of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

This recommendation is based on FERC’s description of EACMs in Order 848, paragraph 54: “*With regard to identifying EACMS for reporting purposes, NERC’s reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. Those functions must include, at a minimum: (1) authentication; (2) monitoring and logging; (3) access control; (4) interactive remote access; and (5) alerting*.”

Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

The only place EAMS is used is in CIP-004 R4 relative to granting physical and electronic access. Please clarify the definition of EAMS. Do EAMS monitor “electronic access” to a BCS or Cyber Asset within a BCS, or does it refer to event monitoring and network inventory discovery tools like SIEMs and Tripwire, Spiceworks, etc? If third party monitoring is allowed, how can the entity timely handle revocation of access? Logging and alerting in CIP-007 R4 refer to EACS however; the proposed definitions do not apply to those terms and are better suited for EAMS.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy agrees with the SDT that there are potential future benefits in separating the control and monitoring functions of EACMS; however, we do not agree these changes should be pursued at this time. It is our view that the changes being considered by the SDT go well beyond the intended scope as provided within the approved SAR. The changes provided by this separation of functions by device, at this time, will again represent another overhaul of existing Entity's CIP programs, processes, and documentation.

Additionally, the current SAR simply asked the SDT to consider how the increased use of virtualization in industry control systems might impact the CIP V5 Standards, along with assessing the security risks associated with virtualization. We do not believe this should be interpreted to mean that the SDT should as a first step recraft the body of CIP Standards in ways that fundamentally change the current BES Cyber System security philosophy. While that may ultimately be what is necessary, we do not believe that is what is required at this time. We are also concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it.

For this reason, we recommend that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, and 3) consideration of how guidance might be developed to assist Responsible Entities who are considering the implementation of virtualization.

Additionally of note, that there are no Parts within the revisions to the Standards that are applicable to EAMS, which would question the need for splitting the EACMS definition versus revising the definition to accommodate the SDT's intent.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CenterPoint Energy) does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

The intent of the new EACS and EAMS terms need to be clarified. The SDT should consider adding “access monitoring, alerting, and logging” to the EAMS definition to be consistent with the approach for PACS and PAMS. The definition should also clarify that the alert is coming from the system generating the alert.	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
This change will require all existing non-third party systems that perform both operations to be re-classified under two Cyber Asset definitions, rather than one. Consider retaining the existing EACMS classification and adding new split classifications that can optionally be used for those systems that only perform half of the functional activities.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 4.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	

Exelon agrees that there are potential future benefits in separating the control and monitoring functions of EACMS; however, we are concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it. More work needs to be done to identify the risk/reward scenarios and what controls would be applied on entity based EAMS vs vendor/cloud based EACS. We also question the backward compatibility of this change, as it drives documentation, compliance tool/technology and process changes. Overall, we do not agree these changes should be pursued at this time and under this effort. It is our view that the changes being considered by the SDT go well beyond the intended scope as provided within the approved SAR. We recommend that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, 3) consideration of how guidance might be developed to assist Responsible Entities who are considering the implementation of virtualization, and 4) consider aligning to NIST or other existing security objective-based frameworks where possible.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "EEI agrees that there are potential future benefits in separating the control and monitoring functions of EACMS; however, we do not agree these changes should be pursued at this time. It is our view that the changes being considered by the SDT go well beyond the intended scope as provided within the approved SAR. Specifically, the SAR simply asked the SDT to consider how the increased use of virtualization in industry control systems might impact the CIP V5 Standards along with assessing the security risks associated with virtualization. We do not believe this should be interpreted to mean that the SDT should as a first step recraft the body of CIP Standards in ways that fundamentally change the current BES Cyber System security philosophy. While that may ultimately be what is necessary, we do not believe that is what is required at this time. We are also concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it.	

For this reason, we recommend that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, and 3) consideration of how guidance might be developed to assist Responsible Entities who are considering the implementation of virtualization."

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Although N&ST appreciates the desire to allow the use of 3rd party monitoring systems in CIP environments, N&ST strongly opposes the idea of allowing “monitoring only” devices to be assigned to a new definition and subject to only CIP-004 requirements. N&ST believes this proposal suggests the SDT considers detective security controls to be of lesser importance than preventative controls, which in our opinion is contrary to generally accepted best practices for layered and multi-faceted cyber security. N&ST notes that the SANS / E-ISAC analysis of the Ukraine power grid attack cites a lack of ICS network monitoring as a likely factor in the attack’s success. N&ST further notes that in FERC Order 850, in which the Commission directs NERC to add EACMS devices to the applicable systems for Supply Chain Standards, the Commission specifically argues against the idea that monitoring may be a less important security function (Paragraph 57).

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6

Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST.

In addition, if an entity is using a single system for both EACS and EAMS, how should the system be identified within CIP-002 (as a EACS, EAMS or EACS / EAMS combination), and should the system be high-water marked within applicable standards and requirements?

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
More clarification is needed regarding the phrase “Cyber System”. The drafting team is proposing a definition of “BES Cyber System”, but there is no definition for “Cyber System”. Is it the drafting team’s intent that an entity should create its own definition for “Cyber System”?	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No

Document Name

Comment

Support MRO NSRF Comments

Likes 0

Dislikes 0

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance

Answer No

Document Name

Comment

LCRA agrees with ERCOT's comment.

Please clarify how an entity would classify an asset that performs and EACS and EAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify - is EAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or is EAMS is to be treated similar to BCSI, which appears to be the case?

Likes 0

Dislikes 0

Response

Robert Ganley - Long Island Power Authority - 1

Answer No

Document Name

Comment

By separating EACMS into EAMS and EACS, it will allow entities to place "monitoring systems" (EAMS) outside of a PSP and be treated similarly to BCSI. While this concept makes sense from an information protection perspective, it dramatically increases risk to the safe and reliable operation of the BES. EAMSs are more than just BCSI containers - they may also perform alerting to potential/actual cyber attacks. Permitting them to reside outside of a defined PSP (refer to EAMS removal in CIP-006-7 Redline) increases the risk of their physical impairment by an attacker. Furthermore, the implementation of EAMSs in either a corporate enterprise or 3rd party environment, potentially outside of a PSP and/or DMZ associated with a LIZ, extends the surface area for a cyber attack and increases the number of potential attack vectors. As a result, it would place BCSs/PCSs at greater risk of an undetected attack.

Since CIP-004-7 continues to include EAMSs in requirements associated with granting and revoking electronic access, the use of 3rd party providers to support EAMSs will become increasingly difficult to manage. 3rd party providers would also have to agree to requirements in other CIP standards such as “disposal of cyber assets containing BCSI”.

If EAMS and EACS functionality cannot be split from a device, it’s unclear as to how it should be categorized. Recommendation: These changes are not impacted by virtualization and should be left as-is.	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
This proposed retirement could have impacts on other Standards, especially CIP-008, that need to be considered.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues. It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.	
Likes 0	
Dislikes 0	
Response	

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	No
Document Name	

Comment

We agree with the split but are concerned of security implications. We request more guidance. Could this approach reduce an Entity's security posture for the sake of meeting compliance? Could this split result in compliance confusion on applicability? How would an Entity correctly classify these assets? We suggest this change drives documentation changes and probably tool/technology changes, so we question this backwards compatibility

We agree that there are potential future benefits in separating the control and monitoring functions of EACMS; however, we do not agree these changes should be pursued at this time. It is our view that the changes being considered by the SDT go well beyond the intended scope as provided within the approved SAR. Specifically, the SAR simply asked the SDT to consider how the increased use of virtualization in industry control systems might impact the CIP V5 Standards along with assessing the security risks associated with virtualization. We do not believe this should be interpreted to mean that the SDT should as a first step recraft the body of CIP Standards in ways that fundamentally change the current BES Cyber System security philosophy. While that may ultimately be what is necessary, we do not believe that is what is required at this time. We are also concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it.

For this reason, we recommend that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, and 3) consideration of how guidance might be developed to assist Responsible Entities who are considering the implementation of virtualization.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends NERC not retire EACMS. Reclamation does not support creating new terms EACS and EAMS. If EACMS must be retired, Reclamation recommends using existing, familiar industry terms (as defined in the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms (NISTIR 7298)).

For example:

Replace **EACMS** with NIST's **Intrusion Detection and Prevention System (IDPS)** – Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Replace **EACS** with NIST's **Intrusion Prevention System(s) (IPS)** – System(s) that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

Replace **EAMS** with NIST’s **Intrusion Detection Systems (IDS)** – System(s) that detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry’s programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to “what to do” not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

If the EAMS contains BCSI then how is third party monitoring allowed? A company still must protect BCSI. More guidance is required for how third party-managed EAMS containing BCSI can be done in a compliant manner. In addition, v5 has an assumption that BCS, PACS, and EACMS are always separate devices. However, they are not. Now we have split EACMS into two along with PACS. So, what is required of devices that have multiple associations? This needs to be address by the SDT.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
NRG asserts that this could have the biggest implication to CIP-004 and CIP-007. This could cause difficulty for the industry to acheive reliability and security due to a broadening of the standards to include serial ports. As an example intrusion detection systems would be required to alert on activity that was not previously configured under the standard.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI agrees that there are potential future benefits in separating the control and monitoring functions of EACMS; however, our members who participated in the development of these comments do not agree that these changes should be pursued at this time. The changes being considered by the SDT go well beyond the intended scope provided within the approved SAR. Specifically, the SAR asked the SDT to consider how the increased use of virtualization in industry control systems might impact the CIP V5 Standards along with assessing the security risks associated with virtualization. However, the SDT appears to be recrafting the body of CIP Standards in ways that fundamentally change the current security philosophy. While that may ultimately be what is necessary, it may not be required at this time to support inclusion of virtualization within the CIP reliability standards. EEI members are also concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it.	

For this reason, EEI recommends that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, and 3) consideration of how guidance might be developed to assist Responsible Entities considering the implementation of virtualization.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
If EACMS is split into EAMS and EACS, what would be considered an EAMS? The camera systems or software used to perform electronic monitoring? CIP-007 and CIP-010 only require Electronic Control Systems (EACS) and no Electronic Monitoring Systems (EAMS). So an entity has to control access but does not have to monitor it, was this the intent of the SDT?	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA	
Answer	No
Document Name	
Comment	

We agree with the split but are concerned of security implications. We request more guidance. Could this approach reduce an Entity's security posture for the sake of meeting compliance? Could this split result in compliance confusion on applicability? How would an Entity correctly classify these assets? We suggest this change drives documentation changes and probably tool/technology changes, so we question this backwards compatibility

Likes 0	
Dislikes 0	

Response
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment
PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0	
Dislikes 0	

Response

5. The SDT realized through the process of splitting EACMS that the same considerations apply to PACS, which will allow changes within the applicability for alerting and logging (PAMS is not reflected within the applicability section at this time). The SDT is considering splitting the PACS term into PACS and PAMS to allow third party monitoring or event correlation to be performed without carrying the PACS classification. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
SMEC agrees with the separation of PACS and PAMS, but there needs to be more guidance provided including how to document cases when they are implemented as the same, or with overlap.	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
LES is in favor of the changes, however we are concerned about the undefined term of "Cyber systems" found in several of the proposed new definitions. LES woudl like to see "Cyber systems" defined.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Please clarify how an entity would classify and asset that performs and PACS and PAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify is PAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if PAMS is to be treated similar to BCSI, which appears to be the case.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
We support a similar approach for PACS as stated in question number 4 above. This will remove any disincentive for additional monitoring of systems.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
We support a similar approach for PACS as stated in question number 4 above. This will remove any disincentive for additional monitoring of systems.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	

We agree that the seperation allows for the utilization of a third party. We have concerns regarding the security controls that will no longer apply to the monitoring systems. This is especially concerning when considering the aggressive timeframes for response to detected conditions.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

Button response should be "No". Editing option seems to be broken.

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

PAC believes this can still be accomplished by maintaining the PACS term and altering the proposed definition. It will allow entities the flexibility to define the different devices that are PACS and what duties they perform. Third party monitoring still fits into the scope of the original definition of PACS. Based on the current proposal of PAMS, there are no instances of the term used in the proposed Standards, it is unclear if this was the SDT's intent.

Proposed change to PACS:

PACS - Cyber Assets [or systems] that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	Yes
Document Name	

Comment

The same comments as the above question 4.

Likes 0	
Dislikes 0	

Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that the same considerations that are applied to EACMS should be applied to PACS.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees.	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern enthusiastically agrees with separating the monitoring/logging aspects out of the access control systems. However, we suggest the SDT consider the need for EAMS and PAMS to exist at all. The monitoring and logging aspects of these systems make any risk they present a data disclosure risk and not a device or system-oriented risk. If the data is of concern, we can have requirements to protect the data without the need for device/system level terms at all. Also, please see our answer to question 4.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
If EACMS is split in two, it makes sense for PACS to also be split.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Please clarify how an entity would classify an asset that performs PACS and PAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify whether PAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if PAMS is to be treated similar to BCSI, which appears to be the case.	
Likes 0	

Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
If EACMS is split in two, it makes sense for PACS to also be split.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	

Document Name	
Comment	
While public power is not sure of the need to separate the terms, if the terms are separated, they will require appropriate accompanying guidance. Consistent with our EAMS response in question 4, clarity regarding applicability of the terms would be needed. The SDT should consider the additional resources and costs associated with a registered entity adding the new applicability to existing CIP-004, R4, and R5 requirements. Moreover, the EAMS and PAMS would need to be incorporated into CIP-011 as designated storage locations. As indicated in the responses to questions 3 and 4, another option is to retain the existing definition while introducing the option to use the new bifurcated formulation, which may offer advantages to some. In this case, the existing PACS term might be re-named PACMS (in parallel with EACMS) so that PACS and PAMS are clear and also parallel to new terms. APPA would also request that the SDT consider the CIP controls appropriate for PAMS. As is the case for EAMS, if defined and scoped carefully, a PAMS may have no 15-minute impact and would not qualify for CIP controls at all, other than potentially as a BCS storage location	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	
abstain	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA	
Answer	
Document Name	
Comment	
abstain	
Likes 0	
Dislikes 0	

Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	
Comment	
Cowlitz supports APPA comment.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
If an entity is using a single system for both PACS and PAMS, how should the system be identified within CIP-002 (as a PACS, PAMS or PACS / PAMS combination), and should the system be high-water marked within applicable standards and requirements? NYPA questions why PAMS is excluded from certain requirements, such as CIP-006 R1.7 (alarm or alert for detected unauthorized physical access) or R3.1 (Maintenance and Testing). If entities rely on PAMS for alerting and logging within CIP-006 R1, these systems should be subject to M&T processes. And if the new definition of PAMS focuses on alerting and logging, this system should be applicable to R1.7. Excluding PAMS from selected requirements is lowering the security bar. In addition, the SDT should justify why PAMS and EAMS are specifically called out within the requirement language of CIP-004 R4.1, 4.4, and 5.3. This approach is inconsistent throughout the standards and exclude other applicable device types listed within the ‘Applicable Systems’ column.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST would oppose this change if it resulted in “PAMS” devices being subject to only CIP-004 requirements (as per our response to Question 4, above).	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "As stated within EEI’s response to Question 4 in consideration of the splitting of the term EACMS, we have similar concerns with the changes being proposed with PACS."	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	

As stated within Exelon's response to Question 4 in consideration of the splitting of the term EACMS, we have similar concerns with the changes being proposed with PACS.

Likes 0	
Dislikes 0	

Response
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 5.

Likes 0	
Dislikes 0	

Response
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	

Comment
Similar to EACMS, this change will require all existing non-third party systems that perform both operations to be re-classified under two Cyber Asset definitions, rather than one. Consider retaining the existing PACS definition and adding new split classifications that can optionally be used for those systems that only perform half of the functional activities.

Likes 0	
Dislikes 0	

Response
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

The intent of the new PACS and PAMS terms needs to be clarified further.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy agrees with the SDT that there are potential future benefits in separating the control and monitoring functions of PACS; however, we do not agree these changes should be pursued at this time. It is our view that the changes being considered by the SDT go well beyond the intended scope as provided within the approved SAR. The changes provided by this separation of functions by device, at this time, will again represent another overhaul of existing Entity's CIP programs, processes, and documentation.

Additionally, the current SAR simply asked the SDT to consider how the increased use of virtualization in industry control systems might impact the CIP V5 Standards, along with assessing the security risks associated with virtualization. We do not believe this should be interpreted to mean that the SDT should as a first step recraft the body of CIP Standards in ways that fundamentally change the current BES Cyber System security philosophy. While that may ultimately be what is necessary, we do not believe that is what is required at this time. We are also concerned that the proposed changes may have many unknown and unintended impacts that could diminish BES Cyber System security rather than improve it.

For this reason, we recommend that the SDT take a more conservative approach through the 1) identification of the security risks introduced by virtualization, 2) consideration of how virtualization might be utilized within the current CIP Reliability Standards structure, and 3) consideration of how guidance might be developed to assist Responsible Entities who are considering the implementation of virtualization.

Given there is no applicability for PAMS at this time, NV Energy would recommend the SDT address the reasoning for maintaining the Glossary Term if its existence is not applicable to the CIP Standards.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

The only place PAMS is used is in CIP-004 R4 relative to granting physical and electronic access. Logging and alerting in CIP-007 R4 refer to PACS however; the proposed definitions do not apply to those terms and are better suited for PAMS.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE shares the same concerns for splitting the PACS term into the terms PACs and PAMs as it does for splitting the EACMS definition. Please see Texas RE's response to #4.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change.   The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

Use of or considering separate systems for control or monitoring for PACS doesn’t seem likely. Therefore, we do not belive the change is warranted.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends the SDT apply the same considerations used for splitting EACMS to PACS. Specifically, Reclamation recommends the SDT consider creating the term PACMS to address existing systems that both control and monitor physical access. Reclamation proposes the existing definition for PACS be used for Physical Access Control and Monitoring Systems (PACMS).

Physical Access Control and Monitoring Systems (PACMS) – Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers

Reclamation supports creating the new terms PACS and PAMS if the PACMS term is also adopted.

Reclamation also recommends changing the proposed definitions of PACS and PAMS to use the term “Cyber Assets” instead of “Cyber Systems,” as described in the response to Question 1,

from:

Physical Access Control Systems (PACS) – Cyber systems that control access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

and

Physical Access Monitoring Systems (PAMS) – Cyber systems that alert or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

to:

Physical Access Control Systems (PACS) – One or more Cyber Assets that control to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

and

Physical Access Monitoring Systems (PAMS) – One or more Cyber Assets that alert or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, cameras, and badge readers.	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	No
Document Name	
Comment	
There is no practical way to meet Requirements related to controlling authorized access without also monitoring whether access granted by the PACS is authorized. In this way, PACS must already be integrated with a form of the proposed PAMS. It is, however, possible for monitoring systems (the proposed PAMS) to go above and beyond the minimum Requirements for PACS. Such additional functionality, which may be helpful to support additional operating controls, should be encouraged. Inventing a new asset class for PAMS would increase the regulatory burden placed on these optional but encouraged systems. The change could have the undesired effect of deterring any monitoring beyond minimum compliance, rather than the desired effect of improving system security.	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	
Comment	
As stated within our response to Question 4 in consideration of the splitting of the term EACMS, we have similar concerns with the changes being proposed with PACS.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No

Document Name	
Comment	
The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues. It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the "how to comply" with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
Similar to our response for Question #4. Recommendation : These changes are not impacted by virtualization and should be left as-is.	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
LCRA agrees with ERCOT's comment.	

Please clarify how an entity would classify and asset that performs and PACS and PAMS functionality. Would high-watermarking to the most restrictive be appropriate? Please clarify - is PAMS is to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or is PAMS is to be treated similar to BCSI, which appears to be the case?	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Support MRO NSRF Comments	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	

Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
The proposed definition of PAMS contains an exclusion for locally mounted hardware or devices as the PSP such as motion sensors, electronic lock control mechanisms, and badge readers. Is it the drafting team’s intent that cameras should fall under the exclusion of locally mounted hardware as well?	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
WAPA does not recommend the splitting of PACS into two separate definitions.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	

Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Industry would need clarity regarding the term PAMS. Does PACS need to be separated into two terms?	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI members who participated in the development of these comments have similar concerns with the changes being proposed with PACS as are described above within EEI's response to Question 4 in consideration of the splitting of the term EACMS.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
In v5 there is an assumption that BCS, PACS, and EACMS are always separate devices. However, they are not. Now we have split PACS into two along with EACMS. So, what is required of devices that have multiple associations? This needs to be address by the SDT.	
Likes 0	
Dislikes 0	
Response	

6. The SDT is proposing to move away from the more prescriptive ESP/EAP model to logical isolation through the higher level objectives provided by the BES Cyber System concept and its Logical Isolation Zone. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
We agree with the concept of logical isolation but struggle with the removal of ERC from CIP-005 R2. Not all substations have ERC and therefore do not have Interactive Remote Access. What are the proposed compliance obligations and what is the best way to demonstrate?	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
We agree with the concept, however LIZ and PCS are defined by their own terms, for example "Logication Isolation Zone: A logicial security zone...." The definitions should be worked on furhter so to avoid this circular definition. This choice of defining also makes 4.2.3.2 and 4.2.3.3 in CIP-010-4 difficult to understand.	
Likes 0	

Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Although N&ST is generally supportive of this proposal, we believe there are significant issues surrounding the question of how compliance, and the use of effective controls, can be adequately demonstrated. N&ST also believes the proposed definition of “LIZ” should be modified, as per our response to Question 12, following.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
While we agree with the proposal to move in this direction, we feel that much more detailed information will be needed in the definitions to fill the void by eliminating the GTB sections. Also, we feel that this approach would benefit from an actual definition for “Logical Security Zone”. This phrase is used in the Logical Isolation Zone definition, but is not itself defined.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
We conceptually agree with proposed definition for Logical Isolation Zone.	
Likes 0	

Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	
Comment	
This is a good move. However, more clarity is needed on the LIZ language to define what the boundaries of an LIZ are. A communication boundary may not be an accurate way to describe the boundary of an LIZ. Traditional definitions of communication do not take into account virtualized systems that share components; information, hardware, and executable code may exist in a location that bridges the communicating boundary of an LIZ. The definition of PCA may need to be expanded to include any asset, such as a hypervisor, that is able to access the internals of an LIZ. For example, if an LIZ includes virtual machines on a VMware host, the host would be a PCA. If an LIZ is containerized, the host OS would be a PCA. If the virtualized assets are on a SAN, then the SAN would be a PCA. The LIZ would need defined limits which are protected by LIZ design. CIP-005 R1.1 would remain necessary and would specify that all applicable BCS must reside within a defined LIZ. The issue would have to be addressed: How to use inclusive language that covers both routable networked devices and components of a virtualized environment, but exclude devices that are neither.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The SDT should consider clearifying the definition of BCS devices to ensure that entities can readily identify the devices and protect them with logical isolation.	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes

Document Name	
Comment	
While AEP agrees, we would like to see examples and/or diagrams of how to apply these zones at a more granular level included in Technical Rationale and or Implementation Guidance.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
This will require the logical isolation rules or policies to be reviewed holistically. Entities will need to thoroughly explain how they are logically isolating and the relation to other networks and systems that are not BCS.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Button response should be "No". Editing option seems to be broken. PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. This term captures the intent, but PAC suggests not using the same words from the term to describe the zone in its definition (i.e. logical security zone = logical isolation zone): Logical Isolation Zone – [delete - A logical] [Electronic] security zone created by applying [logical] controls to communications to or from BES Cyber Systems and Protected Cyber Systems.	
Likes 0	

Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
We agree that this helps allow entities to provide more defense in depth. However, if an Entity has multiple LIZ nested within each other and has a violation of one of the inner LIZ then you have removed the motivation to do more. If an interior LIZ has a violation but is still fully protected by an outer LIZ, then the Violation Risk Factors should reflect that only a violation related to the outer most LIZ of a nested LIZ setup should result in a penalty. However, if all the BCS and PCAs were all protected by another LIZ then the entity should not be penalized for the outermost LIZ violation since they were all within another interior LIZ. This is because the risk to the BES remain unchanged.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Less rigid term, leaves room for circumstances where ESP may have been difficult to be applied.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	

Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Less rigid term, leaves room for circumstances where ESP may have been difficult to be applied.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Hydro One supports the SDT's approach. Assuming all segmentation has to occur at Layer 3 of the OSI stack is doesn't align with current technology trends. We believe that additional implementation guidance is warranted for the industry while allowing flexibility for technical solutions.	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	Yes
Document Name	
Comment	

The SSRG supports retaining the “are connected using a routable protocol” language to provide additional clarity to the definition: LIZ – “A logical security zone created by applying controls to communications to or from BES Cyber Systems and Protected Cyber Systems that are connected using a routable protocol.”	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
While the move to a higher-level view for scoping will require an additional review of our internal programs and lower level work practices, Southern Company believes that this change will allow us additional flexibility in implementing protections at an appropriate level.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
The Technical Rationale document describes well how the Logical Isolation Zone (LIZ) concept will improve the security for virtual environments as well as clarify the serial communications. We recommend that the SDT consider adding clarification to the standard regarding DNP3 over Serial communications. Several questions remain. For example, will the SCADA communications from a front-end processor through a terminal services device to strip off IP communications for DNP3 over serial also be considered as logical isolation? Also, it is not clear why “with External Routable Connectivity” was removed from CIP-005 R2. Given that the CIP-005 Technical Rationale indicates the serial connectivity generally provides logical isolation (p.4), the “with ERC” clarifier should be retained. The LIZ concept represents another dual-definition opportunity, if ESP is retained. An entity would be able select between either concept, on a cyber-system by cyber-system basis, based on which concept makes the most sense for security and operations in its particular environment.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE does not see a need to retire the term ESP and introduce the new term, Logical Isolation Zone. The current definition of ESP provides entities the flexibility to implement ESP(s) based on network environment and technology used. ESP(s) can be established using VLANs, IP ranges, **network zones**, demilitarized zone (DMZ), etc. Changing the definition to Logical Isolation Zone means entities would need to implement “network zones”, which would not allow for the same flexibility as the ESP concept. This could result in potential un-needed upgrades. Texas RE does not agree with retiring the EAP definition. Since network traffic from Logical Isolation Zones will need to pass through an interface, the definition of EAP should be retained and protected how it is currently being protected. Texas RE does agree with moving the concept of PCA to PCS, however, Texas RE recommends using the current definition of PCA and simply change the term to PCS. This is consistent with Texas RE’s recommendation for the BCS definition.	
Likes 0	
Dislikes 0	
Response	

Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO supports the shift from ESP/EAP to a Logical Isolation Zone. MISO requests the SDT consider that inclusion of serial port connectivity may inadvertently expand scope to include devices such as HVAC and physical control locks.	
Likes 0	
Dislikes 0	
Response	

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

NV Energy does not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP), nor do we support their replacement with the newly proposed term Logical Isolation Zone (LIZ). While there may be future benefits to such a change, and NV Energy currently deploys this method of Zone identification within its system, NV Energy does not believe that this is the right time, nor do we agree that the changes being considered will improve an entity's reliability, security and compliance efforts through the higher-level objectives set forth by the SDT. Responsible Entities have broadly built their cybersecurity programs around proven concepts, objectives, and programs. The proposed changes will undoubtedly create significant disruption to those systems and efforts. We also question the need for such broad changes when there are changes within the body of CIP Reliability Standards that will not be enforceable until the year 2020 (e.g., CIP-005-6).

NV Energy is also concerned that the level of change being contemplated by the SDT is too great and represents a very steep learning curve for the industry. For this reason, we ask the SDT to narrow their focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational posting.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

The Logical Isolation Zone (LIZ) concept does not address host firewalls or other technology limiting logical connections to an asset. The SDT should revise the LIZ definition to clarify that the LIZ controls are external to the controls applied by the BES Cyber System itself.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No
Document Name	

Comment

Introduction of a new term logical isolation zone rather than ESP introduces confusion in the definition and with backward compatibility. For example, the definition would now be applicable to serial communications. This is an example of a definition that will be debated for several years in the industry. Continue with our current industry standard definition or ESP and adjust the standards language to address issues or adopt standard NIST terms. SuperESPs can be accommodated by changes to requirements rather than definitions as the current definition of an ESP does not prevent multi-site ESPs.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 6.

Additionally, Westar | Kansas City Power & Light Company share the following observations:

Retiring the Electronic Access Point Glossary Term removes critical identification of the ingress and egress points.

The concept of a Logical Isolation Zone does not relieve the expectation of documented ingress and egress points, especially for network diagramming.

Identify LIZ Data Flow. Related to concerns regarding retirement of the EAP Glossary Term, we believe it is critical that the Logical Isolation Zone considers the ingress and egress flow of data at the zone.

LIZ Residing within a PSP. Considering the Logical Isolation Zone concept, at first glance, it would be expected the LIZ is protected within a Physical Security Perimeter. The LIZ concept is strengthened by an affirmative statement the zone is located within a PSP.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

Exelon does not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP), nor do we support their replacement with the newly proposed term Logical Isolation Zone (LIZ) as part of this effort.

We do agree there may be future benefits to such a change but see this being handled more appropriately within a separate, comprehensive CIP version overhaul effort. Even with the proposed backward compatibility, this change will be disruptive to current CIP programs in place, requiring documentation, compliance tool/technology and process changes. Such a change also brings with it a very steep learning curve for the industry.

We would prefer for the SDT to narrow their focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational comment period.

Likes 0

Dislikes 0

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer No

Document Name

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0

Dislikes 0

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer No

Document Name

Comment

ITC is in agreement with the comments submitted by EEI:

"EEI does not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP), nor do we support their replacement with the newly proposed term Logical Isolation Zone (LIZ). While there may be future benefits to such a change, EEI does not believe that this is the right time, nor do we agree that the changes being considered will improve an entity's reliability, security and compliance efforts through the higher-level objectives set forth by the SDT. Responsible Entities have broadly built their cybersecurity programs around proven concepts, objectives, and programs. The proposed changes will undoubtedly create significant disruption to those systems and efforts. We also question the need for such broad changes when there are changes within the body of CIP Reliability Standards that will not be enforceable until the year 2020 (e.g., CIP-005-6).

EEI is also concerned that the level of change being contemplated by the SDT is too great and represents a very steep learning curve for the industry. For this reason, we ask the SDT to narrow their focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational posting."

Likes 0

Dislikes 0

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC believes the proposed changes to the CIP standards goes beyond the intent of the SAR. The proposed new term LIZ, if approved, should only apply to the virtual devices in which managing access may not use the layer 3 routable protocol while keep the existing requirements the same as before. The changes as proposed will bring BES Cyber Sytems with serial conections, no erc and no dial up into scope for a number of requirements with no benefit. SMEC is concerned that this magnitude of change to the CIP standards and definitions would be too disruptive to non-virtualization compliance.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST. We stress that the SDT must better define the term “communications” used throughout the standards / requirements, and whether this expands the scope beyond routable communications. SDT should also differentiate between a logical and physical environment. The current proposed change does not provide a security benefit and will lead to costly administrative changes (governance documents, asset management systems, diagrams, evidence, etc.). NYPA supports maintaining the ESP / EAP, and routable communication model. In addition, the SDT should consider reverting to the previous CIP-005 R1.1 that required identification (boundaries) of the Electronic Security Perimeter (or Logical Isolation Zone in this case). Entities must define / develop a LIZ before applying required security controls.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	

Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Support MRO NSRF Comments	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP believes removing the term ‘routable protocol’ from the definition may bring serial connections in scope, which are currently excluded. Not excluding serial connection does not allow for backwards compatibility. Additionally, SRP agrees with APPA’s comments.	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
LCRA is concerned that the removal of language specifying the use of a routable protocol may have unanticipated consequences on compliance with requirements where devices were previously not in scope due to not being connected to a BES Cyber System through a routable protocol.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
The exclusion of "Routable Protocol" in the LIZ definition, along with the technical guidance, helps address the use of serial comms and its inherent isolation ability. Note: To achieve this, on CIP-005-7 Part R 1.1, the sub Parts should be bulleted and the “and” between sub Part 1.1 and 1.2 should be an “or”. In addition, it would be preferable to put some specific language in this definition and requirements in lieu of referring to technical guidance. The redaction of EAP from the definition is detracting from the ability to easily identify what connections lead to BCSs/PCSs. Recommendation: Restate EAP definition in new terms that coincide with the implementation of a LIZ. (I.e. Entities can identify “Virtual” EAP’s by name/lable).	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No

Document Name

Comment

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry’s programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

This will require unnecessary additional documentation for serial connected devices. We do not see an issue with the current ESP/EAP model. We support keeping the “are connected using a routable protocol” language.

Likes 0

Dislikes 0

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer No

Document Name

Comment

MEC does not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP), nor do we support their replacement with the newly proposed term Logical Isolation Zone (LIZ). The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0

Dislikes 0

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer No

Document Name

Comment

Recommend changing the label to clarify this is a security label . . . possibly Logical Security Zones

Audit interpretations of this new, more flexible label are a concern

Concern that this does not enhance cyber security, this is not backwards compatible and forces to re-evaluate what is in scope (ie, microwave communications, serial communications, third party communications, etc). Need better clarification on communications demarcation – what is in scope vs out of scope? Concerned that the current CIP-005 R1.1 has not translated well – need more clarity on establishing boundaries and guidance on how to document

We do not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP), nor do we support their replacement with the newly proposed term Logical Isolation Zone (LIZ). While there may be future benefits to such a change, we do not believe that this is the right time, nor do we agree that the changes being considered will improve an entity's reliability, security and compliance efforts through the higher-level objectives set forth by the SDT. Responsible Entities have broadly built their cybersecurity programs around proven concepts, objectives, and programs. The proposed changes will undoubtedly create significant disruption to those systems and efforts. We also question the need for such broad changes when there are changes within the body of CIP Reliability Standards that will not be enforceable until the year 2020 (e.g., CIP-005-6).

We are also concerned that the level of change being contemplated by the SDT is too great and represents a very steep learning curve for the industry. For this reason, we ask the SDT to narrow their focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational posting.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support the proposed term Logical Isolation Zone (LIZ). “Logical isolation” in computer networking is when two sets of devices, which share a physical network infrastructure, are prevented from being able to communicate with each other. The proposed definition implies that a LIZ is a created by *controlling* the communications to and from BES Cyber Systems and Protected Cyber Systems. This is the opposite of isolation.

Logical isolation must distinguish between BES and non-BES. A Logical Isolation Zone could become a risk to BES Cyber Systems when stretched to corporate business enclaves through virtual machine hyper jumping from a lower trust business network. Mixed trust environments on common hardware between CIP Applicable Systems and corporate business networks could also introduce risk to the BES.

Reclamation recommends retaining the existing ESP/EAP model. If the ESP/EAP model must be modified, Reclamation recommends using existing, familiar industry terms (as defined in the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms (NISTIR 7298)).

For example:

Replace **ESP** with NIST's **Enclave** – A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

Replace **EAP** with NISTS's **Enclave Boundary** – Point at which an enclave's internal network service layer connects to an external network's service layer, i.e., to another enclave or to a wide area network (WAN).

Reclamation recommends the following term be added to the NERC Glossary of Terms instead of LIZ:

Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

We disagree to use LIZ to replace the term ESP/EAP that is commonly understood and widely accepted by the registered entities. Given that currently the majority of CIP Cyber Assets (more than 99%) are physical devices and the ESP/EAP compliance process today works fairly smoothly by implementing ESP/EAP requirements that are appropriately prescribed, it doesn't make sense to change ESP to LIZ that is only for sufficing a very small percentage of the virtual devices while ignoring the fact that the majority of physical CIP devices are working very well for the ESP/EAP.

We suggest the proposed new term LIZ should only apply to the virtual devices in which managing access may not use the layer 3 routable protocol while keep the existing requirements the same as before. Resulting from our suggestions, it would be beneficial for all registered entities as follows:

- For the entities that have no any virtual CIP Cyber Assets, they don't need to do anything.
- For the entities that have some virtual CIP Cyber Assets, they may need to use the new term LIZ to resolve the CIP compliance issues unless they could resolve them before.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory

Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to “what to do” not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

This will require unnecessary additional documentation for serial connected devices. The NSRF does not see an issue with the current ESP/EAP model. The NSRF supports keeping the “are connected using a routable protocol” language.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	No
Document Name	

Comment

Cowlitz supports APPA comments and the SDT's intent. The standard language must be adjusted as the current ESP/EAP model will not support virtual systems, but the concerns expressed by APPA should be considered.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

This potential standard change has a broad implication than higher level objectives provided by BES Cyber System concept (and its Logical Isolation Zone). This could cause a re-definition of Interactive Remote Access. This adds a broader compliance burden to the standards than presently required under the non ERC BCA category. The secure configuration now includes serial configuration data. NRG asserts that this potential change would broadly expand confituration data requirements and the controls on configuration of serial ports. Beyond serial implications, it could also impact the 4-20 mA inputs (currently in the standard, implications are for routable communications).

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI members who participated in the development of these comments do not support the proposed retirement of the terms Electronic Security Perimeter (ESP) or Electronic Access Point (EAP) and do not support their replacement with the newly proposed term Logical Isolation Zone (LIZ). While there may be future benefits to such a change, this may not be the right time. We are not currently certain that the changes being considered will improve an entity's reliability, security, and compliance efforts through the higher-level objectives set forth by the SDT. Responsible Entities have broadly built their cybersecurity programs around proven concepts, objectives, and programs. The proposed changes will undoubtedly create significant disruption to those systems and efforts. Further, there is concern on the need for such broad changes when there are changes within the body of CIP Reliability Standards that will not be enforceable until the year 2020 (e.g., CIP-005-6). EEI members are also concerned that the level of change being contemplated by the SDT is too great and represents a very steep learning curve for the industry. EEI recommends that the SDT narrow its focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational posting.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

Logical Isolation Zone poorly defined – because the term "and data" in the proposed BCS Cyber System definition is too ambiguous.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Is it the intent of the SDT that existing ESPs simply convert to a LIZ, where virtual technology doesn't exist? If not, what's the difference between a LIZ and ESP?

We recommend keeping the current ESP/EAP model and the wording in the definitions referencing "routable communication" and "routable protocol connection". In addition, by including serial connected devices in the Requirement, it will require unnecessary additional documentation.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA

Answer	No
Document Name	

Comment

Recommend changing the label to clarify this is a security label . . . possibly Logical Security Zones

Audit interpretations of this new, more flexible label are a concern

Concern that this does not enhance cyber security, this is not backwards compatible and forces to re-evaluate what is in scope (ie, microwave communications, serial communications, third party communications, etc). Need better clarification on communications demarcation – what is in scope vs out of scope? Concerned that the current CIP-005 R1.1 has not translated well – need more clarity on establishing boundaries and guidance on how to document

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

MRO concludes that surface area protection architectures such as the Logical Isolation Zone are not necessarily equivalent or a security improvement when compared to existing perimeter protections. Zone or system level protections such as microsegmentation can enhance the protections provided by perimeter protections, but they are not in conflict with each other and can coexist within the same currently defined CIP environment.

The virtualization changes that are proposed will likely permit mixed some trust applications but it isn't yet clear how logical isolation zones will provide better or equivalent protections to that of an ESP.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

WAPA does not support the proposed term Logical Isolation Zone (LIZ). "Logical isolation" in computer networking is when two sets of devices, which share a physical network infrastructure, are prevented from being able to communicate with each other. The proposed definition implies that a LIZ is a created by controlling the communications to and from BES Cyber Systems and Protected Cyber Systems. This is the opposite of isolation.

Logical isolation must distinguish between BES and non-BES. A Logical Isolation Zone could become a risk to BES Cyber Systems when stretched to corporate business enclaves through virtual machine hyper jumping from a lower trust business network. Mixed trust environments on common hardware between CIP Applicable Systems and corporate business networks could also introduce risk to the BES.

WAPA recommends using existing, familiar industry terms (as defined in the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms (NISTIR 7298)).

- Replace ESP with NIST's Enclave – A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.
- Replace EAP with NISTS's Enclave Boundary – Point at which an enclave's internal network service layer connects to an external network's service layer, i.e., to another enclave or to a wide area network (WAN).

WAPA recommends the following term be added to the NERC Glossary of Terms instead of LIZ:

Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

Likes 0	
Dislikes 0	

Response

7. The SDT is considering taking qualitative language out of the Intermediate System definition and using it to clarify requirements. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Will the Intermediate System extend to the management plane of virtual environments?	
Likes 0	
Dislikes 0	
Response	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Note: the approach taken requires both the definition and details from the requirements to properly understand the location of the Intermediate System relative to the LIZ and other implications.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
While this change is not related to virtualization, the approach does add clarity to the requirements.	
Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

Button response should be "No". Editing option seems to be broken.

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

This term captures the intent, PAC suggests edits to provide additional scoping keeping Intermediate Systems outside of the Logical Isolation Zone they are designed to help protect:

Intermediate Systems - A [cyber] system acting as part of the protection applied [externally] to a logically isolated BCS that limits external user-initiated access to authorized users.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We agree with the proposed definition of Intermediate System. We assume that logical isolation is meant to allow policy based access control

A system acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access to authorized users.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer

Document Name

Comment

Seattle City Light contributed to and supports the comments provided by APPA.

Likes 0

Dislikes 0

Response

Jack Cashin - American Public Power Association - 4

Answer

Document Name

Comment

Public Power is not sure if this changes the function of the Intermediate System. For example, does the Intermediate System still include the, “jump host concept?” Also, it is not clear if the concept extends to management planes or the actual hypervisor. Clarity on these points would be appreciated.

Consider retaining the definition and option to use Intermediate System for entities not pursuing virtualization at this time, and to pilot the new approach with those interested in applying it. This approach will minimize the spread of unanticipated consequences and allow industry and auditors to more gradually learn about the new definitions.

Likes 0

Dislikes 0

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer

Document Name

Comment

abstain

Likes 0

Dislikes 0

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	
Document Name	

Comment

Does the IS have to be inside or outside the LIZ?

Likes 0

Dislikes 0

Response

James Grimshaw - CPS Energy - 1,3,5

Answer	
Document Name	

Comment

Does the IS have to be inside or outside the LIZ?

Likes 0

Dislikes 0

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	
Document Name	

Comment

Cowlitz supports APPA comment

Likes 0

Dislikes 0

Response

David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST. The Intermediate System definition should use “Cyber System” (which needs to be defined) rather than “system.” System is a very broad term and can bring in many devices / equipment currently excluded. In addition, the proposed definition change enables IS to be within the LIZ, which we view as lowering the security bar.	
Likes 0	
Dislikes 0	
Response	

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC does not support the changes being proposed to the term “Intermediate System”, which moves the term from being Cyber Asset based to systems based. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems would be too disruptive to non-virtualization compliance.	
Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST considers the proposed new definition to less clear than the current one, and suggests making only “conforming” changes to the existing definition as needed (such as replacing “Electronic Security Perimeter” with “Logical Isolation Zone”).	
Likes 0	

Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
A missing component of the Intermediate System is the placement of the Intermediate System. Is it the SDT’s intention to allow an Intermediate System to reside within a LIZ?	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "EEI does not support the changes being proposed to the term “Intermediate System,” which moves the term from being Cyber Asset based to systems based. EEI has significant concerns with this al change because it may provide serious issues for both Responsible Entities trying to develop secure solutions and auditors trying to assess entity compliance with the CIP standards. For this reason, we ask that the SDT consider narrowing their focus to addressing specific issues that might negatively impact an entity’s ability to provide necessary protection for BES Cyber Assets within a virtualized environment rather than a complete overhaul of terms and definitions as proposed for this informal comment period."	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

The new definition is unclear and requires more analysis.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

This is too vague and needs background before it can be answered.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

Exelon does not support this change. The new definition is too broad and may introduce some confusion.

We ask that the SDT consider narrowing their focus to addressing specific issues that might negatively impact an entity’s ability to provide necessary protection for BES Cyber Assets within a virtualized environment rather than a complete overhaul of terms and definitions as proposed in this informal comment period.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 7.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
The new definition is unclear and requires more analysis.	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	

The change to Intermediate System brings into question if the authentication servers used to limit access should be Intermediate Systems as well. Additionally, this language appears to make the location (e.g., inside or outside of the firewall) of the IS ambiguous, whereas the existing definition explicitly states that the IS should be located outside of the ESP.

The existing definition is fairly clear and auditors have a clear approach. Consider retaining the existing Intermediate System definition and add a new “Virtual Intermediate System” definition for those entities that wish to pursue that sort of access.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

The Intermediate System definition does not specify that the intermediate system is outside the LIZ. An entity could apply these controls at the BCS level and comply with the standard. The intent is not clear to allow flexibility or require an externally located intermediate system to authenticate users before allowing access to the LIZ and BCS.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy does not support the changes being proposed to the term “Intermediate System,” which moves the term from being Cyber Asset based to systems based. NV Energy has significant concerns with this projected change because it may provide serious issues for both Responsible Entities trying to develop secure solutions and auditors trying to assess entity compliance with the CIP standards.

For this reason, we ask that the SDT consider narrowing their focus to addressing specific issues that might negatively impact an entity’s ability to provide necessary protection for BES Cyber Assets within a virtualized environment rather than a complete overhaul of terms and definitions as proposed for this informal comment period.

Likes 0	

Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO requests clarity on the location of intermediate systems. **Can intermediate systems exist in the same LIZ as other types of CIP Cyber assets, or should they be in a discrete security zone out of a LIZ that contains other types of CIP Cyber assets?**	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry. The NSRF does not see the value in changing the definition. We are concerned that by removing the language, "The Intermediate System must not be located inside the Electronic Security Perimeter." could be construed that an Intermediate System could reside inside an ESP or a LIZ.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	

Answer	No
Document Name	

Comment

Based on our comments on the above, we disagree with the IS definition revisions. The current IS definition is clear and can be applied to the virtual devices as well. As we suggested in the above question 6, the proposed new term LIZ should only apply to the virtual devices in which managing access may not use the layer 3 routable protocol. If SDT wants the IS to apply to LIZ, we suggest revising the IS definition to read (**bold**):

"*A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter* ***or LIZ****.*"

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

The language 'acting as part of the protection applied to a logically isolated BCS…' too broadly scopes the Intermediate System and appears to encompass the definition of an EACS.

Consider changing the proposed Intermediate System (IS) definition to, *A system that limits external user-initiated access to logically isolated BES Cyber Systems for authorized users.* If the SDT does not concur, then BCS to BES Cyber system in the Intermediate System definition should be spelled out.

An Intermediate System is not an applicable system of any CIP requirement. Currently, the EACMS definition includes an Intermediate System in its definition. With the proposed retirement of EACMS the new EACS definition should now say 'this includes Intermediate Systems' in the last sentence of the definition.

Also, the new definition appears to remove the jump-host control from the definition.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support removing the term Cyber Asset from the definition of Intermediate System. Without “Cyber Asset,” the proposed definition of Intermediate System is too broad.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	No
Document Name	

Comment

Concern that this does not enhance cyber security since the Intermediate System could be on the same sub-net as the BES Cyber System

Does the new definition allow firewalls to be Intermediate Systems?

We do not support the changes being proposed to the term “Intermediate System,” which moves the term from being Cyber Asset based to systems based. We have significant concerns with this change because it may provide serious issues for both Responsible Entities trying to develop secure solutions and auditors trying to assess entity compliance with the CIP standards.

For this reason, we ask that the SDT consider narrowing their focus to addressing specific issues that might negatively impact an entity’s ability to provide necessary protection for BES Cyber Assets within a virtualized environment rather than a complete overhaul of terms and definitions as proposed for this informal comment period.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

MEC does not support the changes being proposed to the term “Intermediate System”, which moves the term from being Cyber Asset based to systems based. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	AZPS Comments - Question 7.docx

Comment

Please see the attached document.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry’s programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

We do not see the value in changing the definition. We are concerned that by removing the language, “The Intermediate System must not be located inside the Electronic Security Perimeter.” could be construed that an Intermediate System could reside inside an ESP or a LIZ

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
The revised definition for Intermediate Systems uses the term “system” which is not formally defined. To be consistent, the definition should follow other terminology changes and include PCS. Recommendation: Use the following definition “A combination of one or more cyber assets acting as part of the protection applied to a logically isolated BCS and/or PCS that limits external user-initiated access to authorized users. Intermediate System components must not reside in the same LIZ as a BCS or PCS.”	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The definition of EACMS included explicit language specifying that an Intermediate System was an EACMS. Explicit language or similar guidance should be provided specifying how an Intermediate System should now be categorized. Should it be considered an EACS? LCRA also supports ERCOT’s comment. A missing component of the Intermediate System is the placement of the Intermediate System. Is it the SDT’s intention to allow an Intermediate System to reside within a LIZ?	
Likes 0	
Dislikes 0	
Response	

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

SRP does not see the value in changing the definition. We are concerned that by removing the language, “The Intermediate System must not be located inside the Electronic Security Perimeter” could be construed that an Intermediate System could reside inside an ESP or a LIZ.

Likes 0	
Dislikes 0	

Response

Jamie Prater - Entergy - 5,6

Answer	No
Document Name	

Comment

NERC Proposed: A system acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access to authorized users.

RE Proposed: “A system acting as an intermediatary between protected logically isolated BCS and everything else.”

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Support MRO NSRF Comments

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5

Answer	No
Document Name	

Comment

PSE supports the comments developed by EEI.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO

Answer	No
Document Name	

Comment

Please see MRO NERC Standards Review Forum (NSRF) comments.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy disagrees with the removal of the sentence “The Intermediate System must not be located inside the ESP” from the definition of Intermediate Systems. Was it the drafting team’s intent to remove this phrase, if so, can the team provide its rationale? The concept of Intermediate System has always been understood to mean outside the ESP, but the removal of the language makes this unclear. Also, the proposed definition no longer uses the term “Cyber Asset”, instead uses the term “system”, which seems vague. Can the drafting team clarify what it means by its use of the term “system”?

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

WAPA does not support removing the term Cyber Asset from the definition of Intermediate System. Without “Cyber Asset,” the proposed definition of Intermediate System is too broad.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern is concerned that the use of “to” in the Intermediate System definition may limit the ability of shared account access because of an unintentional scoping created by the word “to” implying that we *must* use individual accounts. Southern Company suggests the following revision: “A system acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access for authorized users only.” In reviewing the use of “to” and “for”, Southern considered: Does using “to” imply a need for an *account* to be authorized, rather than a *user* being authorized?” and “Will using “to” limit our ability to use shared accounts because of an unintentional scoping created by the word “to” implying that we *must* use individual accounts?” Southern would also like to ensure that the term “user” in the resulting definition be preserved as this helps clarify *who* we are talking about (i.e. users, not processes).	

Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	No
Document Name	
Comment	
The SSRG suggests that the potentially vague vernacular “logically isolated BCS” contained in the current definition of Intermediate System could be replaced with “Logical Isolation Zone (LIZ) for added clarity and cross-definition consistency. Also, the way the new definition is structured, one could construe the Intermediate System can be located within the LIZ. The SSRG suggests adding “The Intermediate System should not be located inside the Logical Isolation Zone” to the definition to maintain consistency with the intent of the original definition.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA	
Answer	No
Document Name	
Comment	
Concern that this does not enhance cyber security since the Intermediate System could be on the same sub-net as the BES Cyber System Does the new definition allow firewalls to be Intermediate Systems?	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

The Intermediate System definition "A system acting as part of the protection applied to a logically isolated BCS..." What kind of "protection?" I think it should specify "logical" or "electronic", etc.

Also, we have concerns about the removal of an “Intermediate System must not be located inside the Electronic Security Perimeter” from the definition of Intermediate System. Does this mean we can have an IS inside an ESP?

The more prescriptive language in the current definition does a better job defining an Intermediate System. We recommend keeping the current definition.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI members who participated in the development of these comments do not support the changes being proposed to the term “Intermediate System,” which moves the term from being Cyber Asset based to systems based. This change may cause serious issues for both Responsible Entities trying to develop secure solutions and auditors trying to assess entity compliance with the CIP standards.

EEI recommends that the SDT consider narrowing its focus to addressing specific issues that might negatively impact an entity’s ability to provide necessary protection for BES Cyber Assets within a virtualized environment rather than a complete overhaul of terms and definitions as proposed for this informal comment period.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)

Likes 0	
Dislikes 0	

Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
A missing component of the Intermediate System is the placement of the Intermediate System. Is it the SDT's intention to allow an Intermediate System to reside within a LIZ?	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The proposed new definition implies that if you are using an intermediate system, then you do not have interactive remote access. NRG recommends that the SDT consider leaving the definition as it currently is approved and change the references to the proposed changed terms relating to EACMS.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
While we agree with taking qualitative language of the definition and relocating it to the requirements, we do not believe that the current draft clarifies anything. Instead more questions are raised. For example, an Intermediate System used to have to exist outside the ESP, any ESP. However, can an Intermediate System now exist within a LIZ if it isn't the LIZ of the BCS that it is accessing? Or is this no longer the case and an Intermediate System can now reside within a LIZ? Or, since the Intermediate System is defined as "A system acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access to authorized users," does it mean that the BCS at the end of the remote access connection is actually part	

of the Intermediate System and is thus itself part of an Intermediate System? Especially if the BCS had a host-based firewall acting as a LIZ that helped to limit external user-initiated access to authorized users.	
Likes 0	
Dislikes 0	
Response	

8. The SDT is considering changes to the ERC and IRA definitions to address V5TAG issues (see the CIP-005 Technical Rationale document for detailed information). ERC will have conforming changes only and will continue its use as a scoping mechanism. The proposed modifications to IRA will apply to certain non-routable to routable protocol conversion scenarios. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
It is agreed that the revised definition includes the additional intended scope. The changes to the IRA definition state "...does not include… access initiated from an Intermediate System." It should be made clear in the Intermediate Systems definition that the Intermediate System is an Electronic Access Control System since there is no other clear statement of this. A suggested modification to the Intermediate Systems definition: "An Electronic Access Control System acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access to authorized users."	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
As long as the conforming changes are so that backwards compatibility remains in place.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

SRP agrees with the changes.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We conceptually agree that IRA should apply to the certain non-routable to routable conversion scenarios (serial to IP)

Likes 0

Dislikes 0

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0

Dislikes 0

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jamie Prater - Entergy - 5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	Yes
Document Name	

Comment

Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	

Dislikes 0

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer

Document Name

Comment

Cowlitz supports APPA comment.

Likes 0

Dislikes 0

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer

Document Name

Comment

abstain

Likes 0

Dislikes 0

Response

Jack Cashin - American Public Power Association - 4

Answer

Document Name

Comment

Consider dual parallel definitions, existing and new, for these terms, as discussed above.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE does not see a need to change these terms and notes that changing these terms is not specifically related to virtualization.	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
The Technical Rationale continues to use the term, “ESP.” MISO requests that the SDT redraft the Technical Rationale using the new terminology, “LIZ”, to provide clarity.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy does support the changes to ERC, but does not support the change to Logical Isolation Zone at this time, thus defining our No answer for Question 8 at this time. Additional comments on the Logical Isolation Zone are in our response to Question 6. Additionally, NV Energy understands the intent of the revisions to IRA, but it seems that the access initiated from the Intermediate System is treated as similar to system to system access. In adding certain non-routable to routable protocol conversion scenarios into the concept, the SDT should consider this brings in a huge amount of work for entities.	
Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following: The last clause of the IRA definition “access initiated from an intermediate system” seems contradictory to the intent of using an intermediate system to perform IRA. SDT should consider removing the last clause.	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
CHPD agrees that changes may be needed, but the proposed definition is contradictory to CIP-005 R2, which Part 2.1 specifies that it applies to Interactive Remote Access, but the definition of Interactive Remote Access specifies that sessions from the Intermediate System are not considered Interactive Remote Access. Either this is a misunderstanding of the definition and requirement, which means it is confusing, or a mistake in the definition and requirement. Consider removing “or access initiated from an Intermediate System” from the new IRA definition.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	

More work is needed on these modifications.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 8.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

Exelon views this change as a step in the right direction to clarify what is and is not an IRA. One concern is how this new definition may bring in non-ERC connections under the new definition.

Overall, we do not support the change to Logical Isolation Zone at this time. See comments made in response to Question 6.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
More work is needed on these modifications.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "EEI does not support the change to Logical Isolation Zone at this time. See comments made in response to Question 6."	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	

The modifications to External Routable Connectivity continue to keep the context to being very network centric. This does not address communications that do not use a routable protocol (e.g. fiber channel). This will cause some issues with the implementation of LIZ. Regarding Interactive Remote Access, please clarify the meaning of “access initiated from an Intermediate System”. It is unclear what kind of communication this could be referring to. Please provide clarity on the meaning of “interactive”. Please provide clarity on system-to-system process communication. These have been long-standing issues.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC disagrees with the revisions to ERC and IRA definitions. By removing “with ERC” from the applicable systems column of the requirement tables, multiple requirements will be added to the audit scope that were previously not applicable if there was no ERC. The existence or lack of ERC is fundamental to the current application of CIP Standatrds and removing it will result in additional documentation to prove compliance with no added benefit or reduction in risk.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST. In addition, it’s not clear if the proposed change is limited to routable communications or if this intended to also bring serial / other communication mediums within scope of IRA. This requires clarification.	
Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Regarding the proposal to modify the definition of ERC, Duke Energy recommends that the drafting team take this opportunity to provide needed clarity to the concept of routable protocol (i.e. Would serial to IP convertors be included?). The ambiguity around this topic has led to differing interpretations between entities and regulators. Also, modifications to the term IRA, should include some type of clarification on the concept of system to system communications. This continues to be an issue with varying interpretations.	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	

Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Support MRO NSRF Comments	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
LCRA is satisfied with the ERC definition. The IRA definition is contradictory and confusing. CIP-005-7 R2.1 states 'Have one or more methods to ensure that Interactive Remote Access to applicable systems is through an Intermediate System that is isolated from the BES Cyber System and restricts Interactive Remote Access to only authorized users. The definition of IRA states 'User-initiated access by a person employing a remote access client to a BES Cyber System or Protected Cyber System from outside of a Logical Isolation Zone. Interactive Remote Access does not include system-to-system process communications or access initiated from an Intermediate System.' LCRA would also like clarification on the statement 'remote access client…from outside of a Logical Isolation Zone'. Is this intended to mean access from a client outside of any LIZ or only the LIZ that the destination device is associated with? The previous definition of IRA clarified this issue by stating 'not located within any of the RE's ESPs'. The CIP standard states that IRA must be through an Intermediate System, but the definition of IRA states that it does not include access initiated from an Intermediate System.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for	

what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

We would agree with the changes if LIZ is replaced with ESP in the ERC and IRA definitions.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	AZPS Comments - Question 8.docx

Comment

Please see the attached document.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

MEC does not support the creation of the new Logical Isolation Zone at this time. Therefore, MEC does not support the proposed changes to the ERC and IRA definitions. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	No
Document Name	

Comment

Recommend changing from Logical Isolation Zone to Logical Security Zone

Concern that this change may bring more Cyber Assets into scope

Request more clarity

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation does not support replacing the term Electronic Security Perimeter with the term Logical Isolation Zone (LIZ). Reclamation does not support removing the term Electronic Access Point from the definition of Interactive Remote Access.

If a new term for logical isolation is adopted, Reclamation recommends the following be added to the NERC Glossary of Terms:

Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

Recommend the SDT remove the word ‘connection’ from the ERC definition to ensure it addresses bi-directional routable protocol access opposed to connection. This is consistent with the SDT’s departure from LERC to ‘using a routable protocol’ in CIP-003-7, Section 3.1, ii.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	

Based on our comments on the above, we disagree with revisions of the ERC and IRA definitions. The current ERC and IRA definitions are clear and can be applied to the virtual devices as well. As we suggested in the above question 6, the proposed new term LIZ should only apply to the virtual devices in which managing access may not use the layer 3 routable protocol. If SDT wants the IRA to apply to non-routable for the LIZ, we suggest revising the IRA as follows (**bold**):

“User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol **to pass through ESP or non-routable protocol to pass through LIZ**. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeter(s), LIZ or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.”

If SDT wants the ERC to apply to LIZ, we suggest revising the ERC as follows (**bold**):

The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter **or LIZ** via a bi-directional routable protocol connection.

Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry’s programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to “what to do” not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

The non-routable definition is fundamental to the current understanding and application of CIP standards.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA proposes changing the ERC definition:

Current Proposed: “External Routable Connectivity” is the ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Logical Isolation Zone via a bi-directional routable protocol connection.

BPA Proposed: “External Addressability” is the ability to direct communications traffic to a BES Cyber System from cyber systems external to an entity’s Logical Isolation Zone.

BPA believes this change adequately mitigates the risk of what was formerly known as ERC and allows the scope of controls to exclude communications between secure Logical Isolation Zones. Communications originating inside an LIZ and proceeding to another LIZ are already protected and do not pose additional risk to applicable systems. BPA’s proposed change provides better alignment with IRA requirements and retains better backward compatibility with the current ESP model.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

PacifiCorp’s approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

This term captures the intent, seems that the access initiated from the Intermediate System is treated as similar to system to system access. In adding certain non-routable to routable protocol conversion scenarios into the concept, the SDT should consider this brings in a huge amount of work for entities. PAC would request a 24 to 36 months implementation period for the changes proposed by these revisions.	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
PGE doesn't see that the proposed change in definition have resulted in the desired scope change being applied. Is the proposed definition meant to incorporate the change outlined above? PGE agrees that those types of Interactive Remote Access could benefit from additional security controls.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
The conforming changes for ERC appear to be acceptable. However, if nested LIZ are allowed then consider changing "Logical Isolation Zone" to "Logical Isolation Zone(s)". As for IRA, the proposed changes had setup a dichotomy regarding the protection paradigm of CIP. If user-initiated access by a person employing a remote access client to a BCS or PCA from outside a LIZ, then it appears any access initiated from any LIZ regardless of impact level is acceptable. However, the drafted CIP-005 R3 proposes that further restriction between the data plane and management plane is required. So why is it acceptable to allow any LIZ to LIZ traffic and yet restrict the management plane and data plane? It appears the CIP-005 R3 is accomplished with a LIZ around the management plane. Yet IRA allows LIZ to LIZ traffic, so a CIP paradox has been created and more ambiguity regarding what is allowed and not. This would make the proposed IRA change and proposed requirement changes difficult to audit.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	

Answer No

Document Name

Comment

Not clear whether IRA will apply to non-routable to routable protocol conversion scenarios.

Likes 0

Dislikes 0

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer No

Document Name

Comment

When you remove ERC, you eliminate a threat vector to the ESP. Therefore, the controls required in that situation should reflect that. This proposed standards change reinstates a lot of the controls that were not required under the current version of the standards, which could cause a compliance burden to the industry that may exceed the risk mitigation acheived. NRG asserts that the proposed definition changes to IRA may contradict the requirements relating to CIP-005. The new IRA definition specifically describes that IRA does not include sessions initiated from an intermediate system. As written, registered entities using an Intermediate System, are excluded from CIP-005 R2.

Likes 0

Dislikes 0

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer No

Document Name

Comment

The modifications to External Routable Connectivity continue to keep the context to being very network centric. This does not address communications that do not use a routable protocol (e.g. fiber channel). This will cause some issues with the implementation of LIZ. Regarding Interactive Remote Access, please clarify the meaning of “access initiated from an Intermediate System." It is unclear what kind of communication this could be referring to. Please provide clarity on the meaning of “interactive." Please provide clarity on system-to-system process communication. These have been long-standing issues.

Likes 0

Dislikes 0

Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
Not clear whether IRA will apply to non-routable to routable protocol conversion scenarios.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The EEI members who participated in the development of these comments do not support the change to Logical Isolation Zone at this time. See comments made in response to Question 6.	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
In our opinion LIZ is not a good replacement for ESP. The proposed definition for LIZ doesn't define "communications" or "controls" and results in a definition that is too vague. We recommend keeping the term ESP in lieu of LIZ.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA	
Answer	No
Document Name	
Comment	
Recommend changing from Logical Isolation Zone to Logical Security Zone Concern that this change may bring more Cyber Assets into scope Request more clarity	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	No
Document Name	
Comment	
The SSRG proposes that “system-to-system process communications” should be a defined term that mitigates subjectivity across the industry and provides an objective basis for compliance; and suggests the following definition for “System-to-System Process Communications” could be incorporated: “System to system process communications are communications that are not intiated by a user, but directly by a system to another system with no human interaction.”	
Likes 0	

Dislikes 0

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

User-initiated access by a person employing a remote access client to a BES Cyber System or Protected Cyber System from outside of a Logical Isolation Zone. Interactive Remote Access does not include system-to-system process communications or access initiated from an Intermediate System. Southern requests the SDT consider adding “or other remote access technology using a routable protocol” back in to the definition to retain proper scoping. We do not want KVMs and similar “dumb devices” to be unintentionally scoped in.

Southern would also like clarification on the definition for Interactive Remote Access. While the inclusion of “by a person employing a remote access client” helps clarify that we are discussing people using accounts, this is also implicitly stated later in the definition. Also, including “remote access client” implies that the remote access software be client based and we feel that excluding this will help clarify the scope of the definition.

We propose the following as an alternate IRA definition:

“User-initiated access to a BES Cyber System or Protected Cyber System from outside of a Logical Isolation Zone. Interactive Remote Access does not include system-to-system process communications or access initiated from an Intermediate System.”

Likes 0

Dislikes 0

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

WAPA does not support replacing the term Electronic Security Perimeter with the term Logical Isolation Zone (LIZ).

If a new term for logical isolation is adopted, WAPA recommends the following be added to the NERC Glossary of Terms:

- Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

Likes 0	
Dislikes 0	
Response	

9. To the extent possible, the SDT intends its modifications to permit approaches to compliance that are “backwards compatible” with compliance approaches within the currently approved versions of the CIP standards. (Notable exceptions include CIP-005 R3, CIP-007 R2, and Secure Configurations – CIP-010). Do you agree the modifications are backwards compatible? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST notes that Responsible Entities with no virtualization or limited (no “mixed trust”) virtualization would still be compelled to make extensive (and possibly time-consuming and/or costly) to their CIP evidence files.	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
We agree that the changes appear to be backward compantible, however there are a lot of questions at this point of how comliance will be assessed, especially as we move away from assets toward systems.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Not all entities have adopted virtualization therefore, it is important that terms and concepts remain separated to avoid confusion where there is clearly a separation of physical and virtual environments.	
Likes 0	

Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	
Comment	
The “ERC” qualifier has been removed from CIP-007 R1.1. This could dramatically increase burden on some entities, where the intended effect could be achieved instead with a virtualization-ready definition of “PCA” and “ERC.” CIP-007 R1.4 also seems to shift from requiring intrusion protection on an ESP level to requiring it on a BCS level. This will be onerous and may not be technical feasible in many cases, unless BCS are defined over-broadly (i.e., the entire LIZ is a single BCS). There is a meaningful distinction in keeping the BCS definition separate as a subcomponent of the LIZ. The appropriate shift would be from EAP to LIZ, not from EAP to BCS.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
: NOTE: All references to the new definitions need to be addressed in all the Standards I.e. CIP-009-6 references EACMS an term now being split into EACS and EAMS.	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	

Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
The modifications are backwards compatible, and will proide an increase in security, but they will create more work as the Secure Configuration covers more areas than the current Baseline Configuration.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
The modifications are backwards compatible, and will proide an increase in security, but they will create more work as the Secure Configuration covers more areas than the current Baseline Configuration.	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
PGE has not completed a detailed requirement by requirement analysis but generally believe that these proposed standards provide backwards compatibility.	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	

Document Name

Comment

Seattle City Light contributed to and supports the comments provided by APPA.

Likes 0

Dislikes 0

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance

Answer

Document Name

Comment

No position. No comment.

Likes 0

Dislikes 0

Response

Jack Cashin - American Public Power Association - 4

Answer

Document Name

Comment

Because of the extensive changes to both definitions and Standards, and as a yet-to-be- determined audit approaches, it is not possible, at this time, to be certain that the modifications are indeed backwards compatible. As an alternative that better assures backwards compatibility, consider the option to retain the existing definitions and requirements along with instituting the new definitions and requirements, and then direct entities to select among these two options, on a cyber system basis. This option could be planned to sunset after a set number of years.

Likes 0

Dislikes 0

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	
Document Name	
Comment	
abstain	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE suggests these changes are not necessary as they do not specifically relate to virtualization. These changes appear to be wholesale changes and vastly change the approach of the CIP Standards. Industry just recently went through a large change with the implementation of CIP version 5.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No

Document Name	
Comment	
SMEC appreciates the intent of backwards compatibililty, but the proposed changes will not be backwards compatible for existing compliance documentation. The proposed changes (i.e., removing ESP/EAP, removing BES Cyber Asset definition, etc.) will require entities to change documented processes and compliance evidence for multiple CIP standards. As suggest before, the proposed new term LIZ should only apply to the virtual devices while keeping the existing requirements the same as before. Another alternative would be a new standard which applies only to virtualized systems to address related concerns, thus adding no burden to those entities without virtualization.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The definition of Secure Configuration is recursive and incomplete. The applicability to specific language should not be included in the definition.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "EEI is concerned with the broad changes being contemplated by the SDT. While we applaud the SDT's effort to make these changes "backward compatible" with existing systems not operating within a virtualized environment, the proposed changes system approach introduces new risk to security. We are also concerned that the changes being considered do not take into consideration that the vast majority of systems do not operate within a virtualized environment and are unlikely to be moved in that direction anytime soon. The industry needs more time to better assess the potential disruptive impacts given there are no pressing needs for such changes. More importantly, we cannot say with confidence that the modifications proposed are clearly backward compatible and do not create unintended problems that might compromise BES reliability and security. EEI recommends that the SDT to narrow the focus of this effort to provide clear implementation guidance to protect BES Cyber Systems within virtualized environments under the existing framework already in place."	

Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
We see that a LIZ can be backwards compatible to as ESP, but other changes are not backwards compatible.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
For the most part the current draft presents a systematic approach which is backwards compatible, but Cyber Assets are discrete objects which cannot be systematically removed unless replacing the entire Cyber System. Further CIP-011 contains the term Cyber Asset for disposal and reuse. CIP-011 needs to be modified or further delineation in the BCS definition due to the fact that Cyber Assets, virtual or physical, are still discrete parts of a BCS and cannot be handled systematically.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	

Likes 0

Dislikes 0

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer No

Document Name

Comment

Even with the “proposed backward compatibility,” this change will be disruptive to current CIP programs in place, requiring documentation, compliance tool/technology and process changes. Major changes to our CIP program would be required just to address the foundational definition changes, CIP-002 methodology and assessments, device and asset inventory, patching and change management tools, as well as the entire suite of program, process and procedural documents.

We cannot say with confidence (within this comment period) that the modifications proposed are clearly backward compatible and do not create unintended problems that might compromise BES reliability and security. The proposed changes bring with them a very steep learning curve for the industry.

The timing and scope of these changes is concerning, as they represent a major overhaul of the CIP Standards. We would prefer for the SDT to narrow their focus to providing clear requirements for the protection of CIP systems in virtualized environment, without the broader overhaul of terms and definitions as proposed in this informational posting.

Likes 0

Dislikes 0

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer No

Document Name

Comment

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 9.

Additionally, Westar | Kansas City Power & Light Company share the following concerns.

Recognizing the issue that is being addressed, the strategy “backwards compatible” is ripe with compliance ambiguity and confusion.

The Standards or their revisions are approved and effective at a point in time. That required certainty as to when a Standard is effective is fundamental to compliance and, for that matter, auditability.

Any compelling need to consider “backwards compatibility” can be addressed in Implementation Plans or revisions to the specific Standard. Attempting to address globally will not serve compliance and, in turn, reliability.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	No
Document Name	

Comment

We see that a LIZ can be backwards compatible to a ESP, but other changes are not backwards compatible.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No
Document Name	

Comment

The extensive changes to definitions significantly interferes with practical implementation of the standard in a backward compatible manner.

While on the surface, the changes appear to be capable of being backwards compatible, significant research through a detailed study program is required. Unfortunately, this requires time and the standards are far behind the technology and the increased reliability the new technology provides. A certain component of the backward compatibility will need to be taken on faith. This will need to include modified definitions and guidance that is publicly accepted by NERC as valid.

Clear guidance needs to be created that virtualization that is not mixed mode continues to meet the requirements.

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	

Comment

CHPD is concerned with how this question is asked. The question essentially asks "other than the proposed changes, is the SDT's proposal backwards compatible?" The Secure Configuration concept is such a large deviation from the existing standards that we believe is not valid to exclude it from a question like this. No entity would be able to carry their existing program forward given the sweeping changes proposed, even if they do not intend to virtualize.

The changes to EACMS (splitting into EACS and EAMS) do seem to be largely backwards compatible, so long as you exclude the proposed Secure Configuration concept.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

The proposed CIP-010 language does not address a compliant way to authorize changes after the fact. Previous Requirement R1.2 required change authorization without requiring a timeframe, after the change if necessary. This could be due to operational necessity or minor administrative delay. The new language does not have this flexibility.

The new CIP-007 language requires baselining of all executable scripts. Scripts and "custom" software have been a poorly defined area, but the language in the new standard is broad and therefore difficult to implement or enforce given that any user can enter, execute, and delete scripted commands at a shell prompt. The underlying intent of CIP-007 is a good one, but entities must have the flexibility to automate administrative processes on their own systems, planned or ad-hoc. Furthermore, while installed software or packages are recognized by the OS and can therefore be monitored, scripts are not installed and may not even exist as files. Baselining or alerting on scripts is not practicable.

The new CIP-007 language also requires provision of only "essential" logical access and "essential" software. This is a strong and undefined term. Entities must flexibility to determine what is needed and to revise their determination as their system, or understanding of the system, evolves over time. Language in the new CIP-007 Requirements R1.1 and R2.1 provides no flexibility in revising what is "essential" in a compliant way. CenterPoint Energy recommends that the SDT provide clarification and more context around the term "essential."

Malicious code deterent, detective, or preventative controls may be external to a BCS that cannot run host-based anti-malware controls and therefore cannot be part of the Secure Configuration of the BCS. The NOTE about Secure Configuration should read "The implemented configuration, where implemented on the applicable System, in support of this Part becomes part of the Secure….."

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy would like to praise the SDT’s effort to make these changes “backward compatible” with existing systems not operating within a virtualized environment; however, the proposed changes system approach introduces new risk to security. We are also concerned that the changes being considered do not take into consideration that the vast majority of systems do not operate within a virtualized environment and are unlikely to be moved in that direction anytime soon. The industry needs more time to better assess the potential disruptive impacts given there are no pressing needs for such changes. At this time, NV Energy cannot say with confidence that the modifications proposed, are clearly backward compatible and do not create unintended problems that might compromise BES reliability and security, as this will require additional time and analysis to determine.

NV Energy recommends that the SDT to narrow the focus of this effort to provide clear implementation guidance to protect BES Cyber Systems within virtualized environments under the existing framework already in place.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

MISO does not agree that the changes are backwards compatible. However, MISO recognizes the need for Standards to change as threats evolve and supports the direction of the SDT. Providing clarity regarding the changes and recommendations for proper implementation will facilitate a smoother transition.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

PacifiCorp’s approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

The SDT did a good job here. PAC disagrees with the EACMS and PACS changes and believe we can accomplish the same without the new terms.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3,5

Answer	No
Document Name	

Comment

AEP agrees with modification of Requirements to reduce barriers for increased flexibility and to allow application of new thechnology. However, AEP believes the change from Configuration Baseline to Secure Configuration and additional requirement for risk assessment exceed the mandate from the SAR and will be an unnecessary burden to Industry.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

The NSRF feels there will be significant changes to required documentation.

The MRO NSRF has further concerns the proposed revisions change how to comply but don't improve system reliability or security.

The relatively quick timeframe in which these significant proposed changes were made presents the risk of many unintended consequences for what is the vast majority of systems that are not in virtualized environments. The NSRF agrees that there is a need to take a different approach to Cyber and Physical Security of the Bulk Electric System, however with the continuous state of change and adjustments being made to NERC CIP requirements we do not feel that this is the proper project to take on a larger transformational change.

Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	
The same comments as the above question 6. Given that the CIP compliance process today works fairly smoothly by applying the existing requirements that are appropriately prescribed, any backwards compatible changes have no value for the CIP compliance but wasting the entities' resources for make these changes.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
There are two types of "backwards compatible" – technological and documentational. For entities not employing virtualization, there should be no need to update either the documents or the technologies that refer to ESP and other existing terms. The proposed changes (i.e., removing ESP/EAP, removing BES Cyber Asset definition, changes to EACMS/EACS/EAMS/PAMS/PACS, etc.) will require *all* entities to change their documented processes and compliance evidence for the entire suite of CIP standards.	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	
Comment	

We do not agree that the changes are backwards compatible since existing policies / procedures (system changes, patch management, re-labeling equipment, etc) may need to be re-written and staff will need new training. One example is changing EAP to Logical Security Zone.

Fundamental changes to protection controls which were established CIP Standards version 3.

We are concerned with the broad changes being contemplated by the SDT. While we applaud the SDT's effort to make these changes "backward compatible" with existing systems not operating within a virtualized environment, the proposed changes system approach introduces new risk to security. We are also concerned that the changes being considered do not take into consideration that the vast majority of systems do not operate within a virtualized environment and are unlikely to be moved in that direction anytime soon. The industry needs more time to better assess the potential disruptive impacts given there are no pressing needs for such changes. More importantly, we cannot say with confidence that the modifications proposed are clearly backward compatible and do not create unintended problems that might compromise BES reliability and security.

We recommend that the SDT narrow the focus of this effort to provide clear implementation guidance to protect BES Cyber Systems within virtualized environments under the existing framework already in place.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

We appreciate the intent of backwards compatibility, but are not convinced this will work with the security objective-based requirements subject to different interpretations by Responsible Entities and auditors. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the "how to comply" with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

We disagree that the changes are fully backwards compatible in compliance approach as CIP-004 now includes an access control program for PCS (PCA). There may be many PCA devices within a substation that must be added to the access control program which may require changes to the compliance approach. This may require changes to PCS/PCA controls to bring them into the CIP user authorization program

We do agree that the majority of the changes are backwards compatible from a compliance/ controls approach, but will require extensive documentation changes.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS does not agree that all changes are "backwards compatible" as the proposed modifications are expansive and it is, therefore, difficult to determine with certainty if the changes will generally be backwards compatible. It is also likely that changing definitions that are used throughout all CIP standards will have impacts beyond those immediately obvious, and could affect internal controls.

As an example, AZPS believes the following changes will not be "backwards compatible" and may require extensive changes to internal programs:

- Removal of the term BCA. AZPS has structured its CIP environment to be processed at the BES Cyber Asset level. While AZPS agrees that moving to a BES Cyber System level is appropriate, it will require extensive changes for AZPS to conform its program approach, associated documentation and work processes, associated technology, etc.
- Removal of "routable protocol" from the definition of IRA. This will increase the scope of devices for which compliance with the CIP reliability standards is applicable. Further, this change creates inconsistency by continuing to use "routable protocol" in the applicability tables.

For these reasons, there is a high likelihood that the proposed changes are not wholly backwards compatible and would require a significant effort to revise and implement.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	
Comment	

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

We feel there will be significant changes to required documentation.

Likes 0	
Dislikes 0	
Response	

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	
Comment	

SRP does not agree the modifications are backwards compatible due to the expansion of applicability for various requirements. For example, under the proposed requirement updates, the applicability for CIP-004 R3, R4, and R5 would extend to PCS. If the requirement did not previously apply to certain systems, and the SDT is not following a FERC Order to expand the scope, then SRP does not see a need to expand the applicability of the requirements. In addition CIP-005 R1.2.1 is not backwards compatible as it brings serial port connectivity in scope of the standard and also may indirectly imply encryption on the connections.

Additionally, SRP believes removing the term 'routable protocol' from the definition may bring serial connections in scope, which are currently excluded. Not excluding serial connection does not allow for backwards compatibility.

SRP also agrees with the comments by APPA.

Likes 0	
Dislikes 0	
Response	

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	
Comment	

Support MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

It is difficult to answer the question of backwards compatibility without gaining the necessary clarity on some of the definition proposals. Having said that, it appears at first glance, that certain programmable devices that are considered non-CIP devices (Variable Frequency Drive), would now be considered CIP based on some of the proposed changes. If that is the case, we fail to see how this would equate to backwards compatibility.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company notes concerns with "logical connectivity" in CIP-007 R1.1 below in Q14.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group

Answer	No
Document Name	

Comment

1.) On its face, the SSRG believes the proposal will require significant documentation and system changes to implement and is concerned the modifications are not truly backwards compatable with the current baseline. The SSRG requests the drafting team clarify or explain what the Secure Configuration includes that is not part of the original baseline configuration.

2.) Does the standard drafting team intend the "baseline" paradigm of CIP-010-3 R1.1 to be congruent (i.e., "backwards compatable") with the new "Secure Configuration" paradigm documented in the proposed CIP-010-4 R1.1? In addition, are the controls as documented in CIP-010-4 R1.1.2 indended to be the same as controls as documented in CIP-010-4 R1.2.1. If yes, to avoid confusion and provide specificity to the requirements, the SSRG suggests utilizing corresponding or parallel language in each section where appropriate.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA	
Answer	No
Document Name	
Comment	
We do not agree that the changes are backwards compatible since existing policies / procedures (system changes, patch management, re-labeling equipment, etc) may need to be re-written and staff will need new training. One example is changing EAP to Logical Security Zone. Fundamental changes to protection controls which were established CIP Standards version 3.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
With all the additions, deletions, and revisions to so many terms and definitions it is not possible at this time to be sure of backwards compatibility.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
While the changes appear to be relatively backwards compatible, the items that are required to be part of the Secure Configuration in effect expand the scope of what is required for change control (per CIP-010 R1) in a non-virtual environment. For this reason, we believe the modifications do not appear to be entirely backwards compatible. Tri-State would like to request additional guidance to include an example and a graphic of how backwards compatibility would look for each of the changes.	

Likes 0

Dislikes 0

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3

Answer	No
Document Name	

Comment

Hydro One supports the comments submitted by NPCC TFIST.

Likes 0

Dislikes 0

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI members who participated in the development of these comments are concerned with the broad changes being contemplated by the SDT. These members applaud the SDT's effort to make these changes "backward compatible" with existing systems not operating within a virtualized environment; however, the proposed changes may introduce new risk to security. There is concern that the changes being considered may not take into consideration the vast majority of systems that do not operate within a virtualized environment and are unlikely to be moved into such an environment soon. For these reasons, more time may be needed to better assess the potential disruptive impacts given there are no pressing needs for such changes. As stated earlier, it is not clear that the modifications proposed are clearly backward compatible and concern that the proposed modifications do not create unintended problems and consequences that might compromise BES reliability and security.

To address these concerns, EEI recommends that the SDT focus first on providing clear implementation guidance to protect BES Cyber Systems within virtualized environments under the existing framework already in place.

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
The definition of Secure Configuration is recursive and incomplete. The applicability to specific language should not be included in the definition.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
NRG disagrees with this proposed change because it would cause registered entities to re-assess all aspects of their current NERC CIP compliance programs. An entity cannot be backwards compatible and also achieve the newly proposed requirements. The new secure configuration definition mandates malware monitoring within BES Cyber Systems which implies AV on the BCS and not at the system level (which is the only requirement of the current standard). This proposed change could also imply needing network access control, whitelisting, and/or needing host based intrusion detection.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	

Answer	No
Document Name	
Comment	
PNMR agrees with EEI’s comments. Thank you for attempting to make the changes “backwards compatible.” However, due to the number of definition changes along with requirement changes there are several unintended consequences. Our responses to other questions have brought up only some of the ones that we have identified so far.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Improvements are needed to assure backwards compatibility is retained.	
Likes 0	
Dislikes 0	
Response	

10. The SDT has not yet determined a proposed timeframe to include in the Implementation Plan. How long would you as an entity need to implement the proposed modifications? Please provide your implementation timeframe and justification for why that amount of time would be needed.

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	
Document Name	

Comment

An implementation period would largely be to update documentation and not change technical implementation. A period of 6 months would be sufficient if backwards compatibility is maintained, 12 months minimum for technical implementation changes.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	
Document Name	

Comment

2 to 5 years

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	
Document Name	

Comment

We hesitate to provide an estimate and justification for an Implementation Plan, without gaining the clarity on some of the proposed terms.

Likes 0	
Dislikes 0	

Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	
Comment	
MISO suggests an implementation period of 3 years; the SDT may find it appropriate to design a phased-in implementation with LIZ being in the earlier waves of implementation. Specifically, MISO urges the SDT to clearly define “secure configuration” and/or provide additional guidance on the concept.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	
Document Name	
Comment	
We appreciate the SDTs effort to make the updated requirements backwards compatible but even for an entity that has no virtualization the updated requirements and terms will necessitate re-evaluation of assets, updates to policies and procedures, and implementation of new controls and concepts (for example, the Secure Configuration concept). Based on this alone, we believe that 24 months would be the minimum timeframe required to implement the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	

This Project has made a substantial amount of revisions to the existing CIP Standards, which in turn will require significant overhaul of existing programs and documentation, and at minimum, should require the same implementation timeline that was provided for the CIPv5/v6 implementation.

NV Energy would request a 24 to 36 month timeline for implementation if these revisions are approved.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

18 to 24 months at a minumum. There is great deal of change that will have to be considered, created, and then implemented. The idea presented by some others on phased implementation similar to what was done for V5 also has some merit if it can explained clearly how it can be used and the Regions are willing to accept it.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

CenterPoint Energy suggests the Implementation Plan to be 24 months after Federal Energy Regulatory Commission (FERC) approval. The proposed changes to address virtualization and emerging technologies is significant and a major overhaul of the standards. Entities need sufficient time and resources for implementation and documentation.

Likes 0	
Dislikes 0	

Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	
Document Name	
Comment	
Given the sweeping changes being proposed, CHPD cannot see an implementation period of any less than 36 months. The additional inventory required as part of the Secure Configuration would require this. Additionally, CIP-005 R3 would require network architecture changes that would not be simple to implement.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	
Document Name	
Comment	
Not only will this implementation require adaptation to the new standard, but also restructuring of existing systems with new terminology and re-evaluation of BES Cyber System categorization. This is a widely variable time period depending on size of company. An appropriate implementation plan must allow some type of flexible adoption of the revisions depending on the network and systems considered. For example, an entity not using virtualization may choose to adopt the new standard at a single point in time when language in their systems have been changed. Other entities that are currently using virtualized systems may adopt the new compliance standard at various times for each logical isolation zone that contains virtualized systems. At a minimum, two years will be required at large entities. The radical changes in the standard will cause smaller entities to delay work until the standard is approved by FERC, unless FERC provides some kind of feedback that approval is expected. Again, two years would be the minimum time frame to consider.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	
Document Name	

Comment

18 months

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	
Document Name	

Comment

CIP-005 changes could require extensive architectural changes. This would impact budgets,hardware, software and respective life cycles typically plan three year out. Likewise, The secured configuration management proposed changes could take many years to design and implement.

The proposed changes for EACS/EAMS and PACS/PAMS could be implemented much more quickly with tangible benefits within a year. Likewise, the vulnerability management change could also be implemented relatively quickly.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	
Document Name	

Comment

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 10.

Additionally, Westar | Kansas City Power & Light Company supplements the EEI response with the following detail:

A minimum of three years, likely longer in some instances, to implement the proposed strategy.

To address the proposed revisions / additions to the CIP Standards will require:

- complete review of all systems;
- likely investment in additional or upgraded cyber assets;
- training;
- potentially adding or contracting scarce cyber security engineering expertise; and
- wholesale revision to the company’s CIP processes and procedures.

The proposed strategy will be a substantial undertaking regardless of an entity's size.

Likes 0

Dislikes 0

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer

Document Name

Comment

Seattle City Light contributed to and supports the comments provided by APPA.

Likes 0

Dislikes 0

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer

Document Name

Comment

Due to concerns stated above, Exelon does not support the timeframes included in the Implementation Plan.

A company of our size needs a minimum of three years to make major changes to our CIP program. One year to understand the requirements, agree on a direction for our program and get financing in place; 18 to 24 months to establish the project and deliver; 3 to 6 months to execute, monitor and adapt prior to the compliance enforcement date.

Likes 0

Dislikes 0

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer

Document Name

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0

Dislikes 0

Response

Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6

Answer

Document Name

Comment

18 months

Likes 0

Dislikes 0

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer

Document Name

Comment

We are asking for a 48 month period to implement the proposed modifications. This would allow for programmatic alignment to be accomplished during review cycles, documentation alignment and review, and additional time to align process and procedures.

Likes 0

Dislikes 0

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer

Document Name

Comment

CIP-005 changes could require extensive architectural changes. This would impact budgets,hardware, software and respective life cycles typically plan three year out. Likewise, The secured configuration management proposed changes could take many years to design and implement.

The proposed changes for EACS/EAMS and PACS/PAMS could be implemented much more quickly with tangible benefits within a year. Likewise, the vulnerability management change could also be implemented relatively quickly.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"Due to concerns stated above, EEI does not support the timeframes included in the Implementation Plan."

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	
Document Name	

Comment

24 months is needed at a minimum. Entities need to reevaluate technologies currently used to manage processes supporting compliance to the requirements. This is particularly important with transitioning from patch management to vulnerability management. This will most likely require capital investments which require adequate budget time.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES

Answer	

Document Name	
Comment	
24 months.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	
Document Name	
Comment	
N&ST believes the proposed modifications represent a significant change to the CIP Standards. Based on that opinion, N&ST believes the implementation time frame should, if all proposed modifications were approved, be at least 24 months.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	
Document Name	
Comment	
3-5 years	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	

Twelve months as the proposed changes are backwards capatible and our current protections for virtualized systems align perfectly with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	
Document Name	
Comment	
PSE supports the comments developed by EEI.	

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	
Document Name	

Comment

Support MRO NSRF comments

Likes 0	
Dislikes 0	

Response

Jamie Prater - Entergy - 5,6

Answer	
Document Name	

Comment

3-5 years

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

SRP recommends including an additional 36 to 48 months in the Implementation Plan because the new terminology and retired terminology are now in more requirements creating a review and revision administration burden. This will allow Responsible Entities time for planning, budgeting, and evaluating new tools, hardware, software, professional services, architectural changes, and encryption.

Additionally, the suggested changes increase the scope substantially by including serial connectivity and applicable devices into requirements they were not previously in. This is an overhaul of the CIP standards just as with version 3. SRP also requests the time frame between the current standards and the standards with the revised methodology be treated as the CIPv3 to v5 transition.

SRP also agrees with APPA's comment regarding a pilot program.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance

Answer	
Document Name	

Comment

LCRA proposes a 24 calendar month timeframe to implement the proposed changes. Some changes to the standards, such as those related to Secure Configuration, will require testing on how to best implement the requirements for LCRA's BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	
Document Name	

Comment

3-5 years would be required to address (document, fund and implement) significant changes to systems that will support the new requirements (i.e. CIP-007 R2).

Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	
Document Name	

Comment	
18 - 24 calendar months. This would allow entities time to redo their processes and properly address the risk based language that has been included. It would also allow some technical changes to occur for new or revised requirements (i.e. data communicaiton encryption, etc.). Additionally, it would be beneficial to have the option for entities to adopt the revised requirements early, once approved by FERC, similar to how CIP Version 5 was implemented.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	
Document Name	
Comment	
NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations. We do not agree with most of the changes, especially the removal of BCA and ESP. If the changes were to go through as proposed we would request a minimum of 24 months due to architecture redesign, documentation updates, and documentation review.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	
Document Name	
Comment	
AZPS respectfully requests consideration of a 30-month implementation plan timeframe given the wide breadth of change required.	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Three years because this change is similar in scope to upgrading from CIP version 3 to 5. We suggest borrowing from that earlier implementation plan, where each Entity had the option of which version to adhere to and by BES Cyber Asset / BES Cyber System (instead of wholesale conversion).	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
We propose a three years timeframe since this change is similar to when CIP version 3 was upgraded to version 5.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	
Document Name	
Comment	
If NERC and FERC approve such wide-sweeping changes, industry will need at least as much implementation time as was provided for CIP version 5 to overhaul all CIP programs and retrain personnel and practice on all standards before the effective date. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the	

existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	
Document Name	

Comment

Three years because this change is similar in scope to upgrading from CIP version 3 to 5.

We suggest borrowing from that earlier implementation plan, where each Entity had the option of which version to adhere to and by BES Cyber Asset / BES Cyber System (instead of wholesale conversion).

Likes 0	
Dislikes 0	

Response

Joseph Pride - Trans Bay Cable LLC - 1 - WECC

Answer	
Document Name	

Comment

Two years. As described elsewhere in this response, the proposed changes blur the line between what constitutes a Logical Isolation Zone and a BES Cyber System, now applying Requirements at the BCS level that previously applied only to an EAP or an ESP with ERC. Depending on the system, these changes could require a combination of major technical enhancements on a BCS level and the administrative burden of restructuring what constitutes a BCS. The changes could be more backward-compatible, and therefore faster to implement in most cases, if network-level protections are applied to the Logical Isolation Zone while system-level protections are applied to the BCS. The proposed isolation of the Management Plane from the Data Plane could be more backward-compatible if its application scope is refined to only those assets where the Management Plane would be capable of changing the isolation limits or accessing internal data from outside of a Logical Isolation Zone, for which we propose the new term “Zone Boundary System.”

Likes 0	

Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
Reclamation recommends the SDT consider separate, 24-month phased-in implementation plans for each affected CIP standard to avoid numerous changes becoming effective on the same date. This will allow entities time to determine the effects of the revised requirements and definitions, develop adequate written processes, and train personnel appropriately. Reclamation suggests the SDT consider a longer implementation schedule for entities that use virtualization (e.g., an additional 18 months) than for those that don’t.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
Minimum 24 months. Entities are adapting to the new terms and mapping backward compatibility. The terms used require piloting in operational environment to highlight implementation difficulties. The extra time also smothes out work burden to avoid overload of existing staff levels.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	

Comment

18 months is needed to ensure….

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	
Document Name	

Comment

We disagree with most of the proposed changes except EACMS and PACS.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There is also multiple registered groups who can write and submit to NERC, Implementation Guidance. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtuazation practices under our current set of Standards. All Standards are written to “what to do” not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still do not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

We do not agree with most of the changes, especially the removal of BCA and ESP.

Industry needs 4 calendar years or 48 months to adequately design, spec, budget, build, implement, rewrite program documents and train on all of the new requirements. Each one of these phases takes time to implement.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

BPA points out that with the definition changes it will be impossible to utilize a phased implementation approach; therefore we predict a long implementation period will be necessary for most entities. Transition to the new version should be allowed prior to mandatory and enforceable date.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3,5

Answer	
Document Name	

Comment

AEP believes systems changes and process changes to account for classifications and changes to definitions would require at least 24 months to implement or longer if requirements to assess risk as proposed in CIP-010-4 are retained.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
: PacifiCorp’s approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. PAC would request a 24 to 36 months implementation period for the revisions proposed.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	
Document Name	
Comment	
2-5 years due to small public entities with limited staff and resources. These entities must first budget through the approved budget that is not as fexible as larger agencies. This includes public meetings and voting by publicly elected officials. Typically, one FTE is a significant expense and must be well supported. Additonal systems, equipment and processes take considerable resources in small organiztions. Repetative work loads must also me considered for staffing purposes at smaller agencies. Physical and Cyber Security has been one of the single bigest cost drivers in small agencies and has begun to negatively impact rural ratepayers, especially in depressed economies that still struggle to get basic services.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have a comment on this question.	
Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	
Document Name	

Comment

Cowlitz supports APPA coments.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro

Answer	
Document Name	

Comment

BC Hydro’s assessment is that, due to the scope of this assessment on the BC Hydro systems, at least 24 calendar months would be required to analyze the full impacts of the proposed modifications.

Likes 0	
Dislikes 0	

Response

Nathaniel Clague - Portland General Electric Co. - 1,3,5,6

Answer	
Document Name	

Comment

PGE would propose a minimum of 24 months for implementation of the new standard. PGE would also suggest guidance for entities and auditors alike on how to make the transition as seamless as possible. The ability to transition early for those entities that wish to take advantage of the flexibility allowed in the standard should be addressed.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer

Document Name

Comment

It is unclear if the proposed modifications could even be successfully implemented to be auditable with just some of the concerns raised in our other comments. Without more time to process these changes and ramifications, we cannot even guess as to how long we would need to implement the proposed modifications.

Likes 0

Dislikes 0

Response

James Grimshaw - CPS Energy - 1,3,5

Answer

Document Name

Comment

2 years (budgetary reasons, training, reconfiguration of systems, compliance with Secure Configuration, risk analysis, etc.)

Likes 0

Dislikes 0

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer

Document Name

Comment

NRG asserts that registered entities would require at least 24 months to implement these technical changes to account for a design, budgeting, and implementation cycle. NRG asserts that registered entities would require at least an additional 12 months to train and adapt personnel to procedural changes for a total of three years implementation [similar to a V3 to V5 transition].

Likes 0

Dislikes 0

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer

Document Name

Comment

24 months is needed at a minimum. Entities need to reevaluate technologies currently used to manage processes supporting compliance to the requirements. This is particularly important with transitioning from patch management to vulnerability management. This will most likely require capital investments, which require adequate budget time.

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer

Document Name

Comment

Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)

Likes 0

Dislikes 0

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer

Document Name

Comment

2 years (budgetary reasons, training, reconfiguration of systems, compliance with Secure Configuration, risk analysis, etc.)

Likes 0

Dislikes 0

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3

Answer

Document Name

Comment

Hydro One supports the comments submitted by NPCC TFIST.

Likes 0

Dislikes 0

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC

Answer

Document Name

Comment

BHP anticipates it would take eighteen to twenty-four months to implement these changes.

Likes 0

Dislikes 0

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer

Document Name

Comment

Tri-State recommends an implementation timeframe of 24 months after approval by FERC. This will give entities time to understand the changes to the standards and then design, test, and implement program changes.

Likes 0

Dislikes 0

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	
Document Name	

Comment

Recommend at least 36 months to perform architecture redesign, documentation updates, and documentation reviews.

Dial-up is employed at many locations throughout our company and a significant amount of work will need to be completed to meet the requirements in the Standard especially with the removal of ERC, BCA, and ESP from the Standards. In addition, budgets are completed annually so if additional equipment is required it would need to be included in annual budget cycles.

Because of the extensive amount of changes currently proposed we recommend a NERC sponsored pilot program similar to what was done for CIP Version 5.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA

Answer	
Document Name	

Comment

Three years because this change is similar in scope to upgrading from CIP version 3 to 5.

We suggest borrowing from that earlier implementation plan, where each Entity had the option of which version to adhere to and by BES Cyber Asset / BES Cyber System (instead of wholesale conversion).

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group

Answer	
Document Name	

Comment

The SSRG suggests 24 months to ensure adequate artchitechture design, documentation updates, and documentation review.

Likes 0

Dislikes 0

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer

Document Name

Comment

abstain

Likes 0

Dislikes 0

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer

Document Name

Comment

Given that these changes will require Responsible Entities to review internal program documentation and potentially make signification changes to their programs, 36 months is a reasonable timeframe for successful implementation of the necessary changes. The changes required for internal program documentation and coordination of these changes across large enterprises will take time to develop and implement. For Registered entities that choose to shift from an asset-based CIP philosophy to a system-based one, the change of alignment will be a significant program change. Changing configuration management from our current methodology (logical to system or system to logical) will take significant time to change and also what and how we gather the required evidence to demonstrate compliance. Enumerating the change will require new processes. New processes will take time to implement.

Likes 0

Dislikes 0

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer

Document Name

Comment

PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0

Dislikes 0

Response

sean erickson - Western Area Power Administration - 1,6

Answer

Document Name

Comment

24 months

Likes 0

Dislikes 0

Response

Jack Cashin - American Public Power Association - 4

Answer

Document Name

Comment

At a minimum, APPA recommends that the timeline for the Implementation Plan be 24 months. Public power companies believe Virtualization will be a challenge that will exceed the transition from CIP Version 3 to Version 5. Implementation will require significant time and resources. Consequently, sufficient time and an appropriate compliance approach will be needed to ensure successful implementation.
Because of the extensive, untried nature of the changes, we strongly urge a NERC-sponsored pilot program with volunteer entities, analogous to that undertaken for the CIP v5 changes.

The implementation timeline might be minimized under a “virtualization overlay” approach, in which entities can elect to stay with existing definitions and requirements or move to the new ones (on a cyber-system by cyber-system basis). Perhaps 12 or 18 months might suffice in such a case, which would allow interested entities to exploit as soon as possible the possibilities of virtualization.

Likes 0

Dislikes 0

Response

11. The SDT is proposing conforming modifications to CIP-004. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. Modifications related to CIP Exceptional Circumstances

b. Use of newly proposed terms EACS and EAMS in the Applicable Systems column

c. Addition of PCS to the Applicable System column for Parts in CIP-004 to mitigate security risks associated with individuals not needing authorization or PRAs when granted access to systems inside the Logical Isolation Zone

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	Yes
Document Name	

Comment

SMEC agrees with modifications related to CIP Exceptional Circumstances. SMEC believes further guidance should be provided to define the split of EACMS.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	Yes
Document Name	

Comment

We are in agreement with the changes related to CIP Exceptional Circumstances, the use of the newly proposed terms EACS and EAMS, and the addition of PCS. However, we believe it would also be prudent to include PCS under CIP-004 R2. Individuals who have access to PCS have access to systems inside the LIZ and should be trained on the security risks accordingly.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	Yes
Document Name	

Comment	
We support the changes related to the EACMS and PACS. As we suggested in the above question 6, the LIZ should only apply to the virtual devices in which managing access may not use the layer 3 routable protocol.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
a. The modification to CEC is appropriate for CIP-004. b. There are concerns around revocation of access in a timely fashion if a third party service is used for monitoring of EAMS and PAMS. c. The definitions for Protected Cyber Systems and Logical Isolation Zone lose the "routable" distinction for communications. This is somewhat addressed in CIP-005-7 1.2.1, but recomend it remain in the definition. Also, the LIZ definition doesn't define "communications" or "controls," so exactly what will define this zone? A modem can be said to "control communications." The definition of LIZ is too vague.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
Button response should be "No". Button selection wasn't allowed. PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. The SDT did a good job here. PAC disagrees with EACMS and PACS changes and believe we can accomplish the same without the new terms. If the PCS is going to be added to the R3 applicability is should be added consistently to CIP-004 and be added to R2.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	

APPA believes the modifications to CIP Exceptional Circumstances (CEC) are appropriate. However, the SDT needs to verify that standards being balloted separately (CIP-008 for example) are considered and included appropriately for CEC. This is especially important for CIP-008 given that the definition of CEC includes language on Cyber Security Incidents.

The only place that EAMS and PAMS appear in the revised standards is under requirement language in CIP-004 R4 and R5. Public power believes that the CIP-004 update does not alleviate third party provider concerns with PAMS and EAMS. See discussion under Question 4.

Public power does not agree with the expansion of applicability for CIP-004 R3, R4, and R5 to include PCS. Changes in these Applicability Systems are not consistent with this Standard’s Purpose statement.

If PCAs were not included originally and the SDT is not following a FERC order to do so, then there is no reason to make them applicable. In CIP-004, R4, and R5 the terms EAMS and PAMS are selectively included in the Requirement language.

In general, the necessity to expand the scope of CIP Standards to address new vulnerabilities introduced by virtualization can be minimized or eliminated by use of the dual-definition/parallel requirement “virtualization overlay” approach discussed above.

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	
Document Name	

Comment

Cowlitz supports APPA comments.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

a. Texas RE agrees with the addition of the CIP Exceptional Circumstance language to proposed CIP-004-7 R3, Part 3.5.

b and c. Please see comments in question #4 related to the applicability of ECMS and EAMS. If the industry wants to revisit the applicability of the requirements to various systems, Texas RE recommends this be done in a separate project where a standard drafting team can perform a holistic review of all CIP standards.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST agrees with modifications related to CIP Exceptional Circumstances and addition of PCS to certain Parts in CIP-004. However, N&ST objects to the proposal to make newly-defined EAMS and PAMS subject only to CIP-004 (as per our response to Question 4).	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	

Please clarify if EAMS and PAMS are to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if EAMS and PAMS are to be treated similar to BCSI, which appears to be the case. If they are intended to be treated similar to BCSI, they should not be included in the applicable systems column. They should only be in the requirements column. The periodic review requirements need to be clarified based on the intent. As written, you are requiring quarterly review of BCSI-like repositories. You are also requiring two different types of access reviews every 15 months. This seems duplicative and inappropriate. The same issues are present with the access revocation tasks under Requirement R5.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	No
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"Although EEI does not agree with the modifications related to CIP-004 as described above, we do support the modifications to the CIP Exceptional Circumstances. Also, we do not support the modifications to the proposed retirement of EACMS, ESP, EAP, etc. for the reasons previously stated in our comments."

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	
Comment	

Although Exelon does not agree with the modifications related to CIP-004 as described above, we do support the modifications to the CIP Exceptional Circumstances. Also, we do not support the modifications to the proposed retirement of EACMS, ESP, EAP, etc. for the reasons previously stated in our comments.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	
Comment	

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 11.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No
Document Name	
Comment	

Yes – CIP Exceptional Circumstances

No – EAMS and EACS

Yes – Addition of PCS

Disagree with the use of EAMS and PAMS in the applicable systems column. One significant issue that is being studied is the use of cloud storage and the use of remote monitoring by professional services firms that have higher levels of security skill than many entities. By including EAMS and PAMS in CIP-004 requirement part 4.1, this difficulty is perpetuated.

In its place, Wabash Valley recommends a new CIP-004 requirement part governing for access to EACS, EAMS, PACS, PAMS, governing electronic access, physical access, and BCSI Storage location access to:

Identify and demonstrate that access controls have been implemented by the entity or through implementation of a widely accepted independently audited certification such as ISO 27001, FEDRAMP, <Canadian Equivalent to FEDRAMP> or <Mexican Equivalent to FEDRAMP>.

May need to add an additional part or language to address the case of a withdrawn certification.

Likes 0

Dislikes 0

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer No

Document Name

Comment

NV Energy does not agree with the majority of the modifications related to CIP-004 as described above, however, NV Energy does support the modifications to the CIP Exceptional Circumstances. Also, we do not support the modifications to the proposed retirement of EACMS, ESP, EAP, etc. for the reasons previously stated in our comments.

NV Energy believes that the revisions to the definitions are unnecessary at this time, and can be addressed through correct identification of PCA within the existing CIP Standards language.

Likes 0

Dislikes 0

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer No

Document Name

Comment

MISO supports the shift to EACS and EAMS. MISO encourages the SDT to reinforce the differences between the security requirements for the monitoring and the access functions.

Likes 0

Dislikes 0

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	
Comment	
If a device is classified as an EAMS or PAMS, does that require the device to be considered a BES Cyber System Information storage location? What about third-party hosted EAMS/PAMS and the implications to CIP-004 controls?	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
The addition of PCS to CIP-004 increases the documentation burden to entities who will now have to identify additional systems and those who have access. Documentation of access to a BCS and LIZ should suffice and imply access to associated PCS.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
If the stated intent of the creation of EAMS is “to allow third party monitoring systems” and PAMS is “to allow third party monitoring or event correlation”, BPA believes this is not specifically supported in the requirements CIP-004 R4.1/4.2 since CIP-004 R4.2 directs “Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.” If the intent is to allow third part monitoring, there needs to be a way to allow authorization on a vendor or provider basis. BPA suggests this could be done via contract language or grant to that company. This exists in CIP-004 R5.1, 5.2, 5.3 and anywhere else action on an individual basis is required.	
Likes 0	
Dislikes 0	
Response	

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

a. Reclamation agrees with the modifications related to CIP Exceptional Circumstances. CIP Exceptional Circumstances are necessary during emergencies for first responders.

b. Reclamation disagrees with the proposed terms EACS and EAMS in the Applicable Systems column. Reclamation recommends the SDT use Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) instead, as stated in the response to Question 4.

c. Reclamation agrees with the addition of PCS in the Applicable Systems column for CIP-004; however, Reclamation does not agree with the proposed PCS definition. The system wide approach does not allow for the detail needed to properly address all security issues.

Reclamation recommends changing the PCS definition

from:

Cyber systems that can communicate with a BES Cyber System from within the BES Cyber System's Logical Isolation Zone. The impact rating of Protected Cyber Systems is equal to the highest rated BES Cyber System within the Logical Isolation Zone.

to:

One or more Cyber Assets that can communicate with a BES Cyber System from within the BES Cyber System's Electronic Security Enclave. The impact rating of Protected Cyber Systems is equal to the highest rated BES Cyber System within the Electronic Security Enclave.

Likes 0

Dislikes 0

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer No

Document Name

Comment

Recommend changing from Logical Isolation Zone to Logical Security Zone

Changes in these Applicability Systems are not consistent with this Standard’s Purpose statement

Changes to Applicability Systems in 4.2 – 4.5 and 5 increase the workload. This increase will negatively affect focus on BES Cyber Systems with a decrease in cyber security effectiveness

This CIP-004 update does not alleviate third party concerns with PAMS and EAMS. Should CIP-005, CIP-006, CIP-007 and CIP-010 have matching updates.

In CIP-004, R4 and R5 the terms EAMS and PAMS are selectively included in the Requirement language. Request clarification since these systems are already included in the Applicable Systems column.

Request clarification on CIP Exceptional Circumstances because there is some confusion. Some changes are the main Requirement level. Others are at the sub-Requirement level. Expected all these changes at the main Requirement level.

Likes 0

Dislikes 0

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer No

Document Name

Comment

MEC does agree with some of the modifications related to CIP Exceptional Circumstances, such as adding it back to CIP-004-6 R3, but we do not agree with the conforming changes resulting from the retirement of EACMS, ESP, EAP, etc. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

a. We conceptually agree to the proposed changes for CIP Exceptional Circumstances.

b. We conceptually agree to the proposed changes for EACS and EAMS.

c. We conceptually agree with the addition of PCS into the access control program in CIP-004 however at the substation level, there may be technical issues in applying the same access controls program to all existing PCS devices.

This may require wording “per PCS capability” or similar into some CIP-004 requirements

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

a. Agreed

b. Proposed definitions need to be re-evaluated.

c. Agreed with the following caveat; that read-only systems that are currently viewed as IRA requiring intermediate systems should be excluded or handled differently.

Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP does not agree with the expansion of applicability for CIP-004 R3, R4, and R5 to include PCS. If PCAs were not included originally and the SDT is not following a FERC order to do so, then SRP does not see a need to add them to the applicability. SRP also agrees with APPA’s comments.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Support MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	

Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company agrees with the CEC additions and with the addition of PCS to the applicability of these requirements. However, we disagree with the inclusion of EAMS and PAMS throughout R4 and R5. Southern asserts that retaining EAMS and PAMS on these requirements prevents the results the SDT has stated as reasons for splitting these terms. Entities will still not be able to utilize vendor or government agency services that can enhance reliability and security and help detect cyber-attack activity early in the kill chain if we shackle the entities with requirements on the personnel or devices/systems at those outside entities. We suggest the SDT consider the need for these terms at all. Can government “cloud service” certification (FedRAMP, etc.) help achieve the same data security end goal when external parties are involved? If the three letter government agencies can certify against a government body (FedRAMP), we assert that we should be able to do the same.	

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

abstain

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA

Answer	No
Document Name	

Comment

Recommend changing from Logical Isolation Zone to Logical Security Zone

Changes in these Applicability Systems are not consistent with this Standard’s Purpose statement

Changes to Applicability Systems in 4.2 – 4.5 and 5 increase the workload. This increase will negatively affect focus on BES Cyber Systems with a decrease in cyber security effectiveness

This CIP-004 update does not alleviate third party concerns with PAMS and EAMS. Should CIP-005, CIP-006, CIP-007 and CIP-010 have matching updates.

In CIP-004, R4 and R5 the terms EAMS and PAMS are selectively included in the Requirement language. Request clarification since these systems are already included in the Applicable Systems column.

Request clarification on CIP Exceptional Circumstances because there is some confusion. Some changes are the main Requirement level. Others are at the sub-Requirement level. Expected all these changes at the main Requirement level.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
Tri-State requests rewording of the Requirements R4.1.3 and R4.4 to clarify if it is the the access type or reposity type that is qualified with "physical or electronic." For example, is physical access in scope for electronic repositories?	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
In agreement with BPAs comment - If the stated intent of the creation of EAMS is "to allow third party monitoring systems" and PAMS is "to allow third party monitoring or event correlation", BPA believes this is not specifically supported in the requirements CIP-004 R4.1/4.2 since CIP-004 R4.2 directs "Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records." If the intent is to allow third part monitoring, there needs to be a way to allow authorization on a vendor or provider basis. BPA suggests this could be done via contract language or grant to that company. This exists in CIP-004 R5.1, 5.2, 5.3 and anywhere else action on an individual basis is required.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST.	

Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Although the EEI members who participated in the development of these comments do not agree with all of the modifications related to CIP-004 as described above and do not support those modifications to implement the proposed retirement of EACMS, ESP, EAP, etc., EEI does support the proposed modifications to the CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
The exception should be for prior to granting authorized electronic access and authorized unescorted physical access to align with R2.2 training and Part 4.1 process to authorize based on need. Additionlly, if PCS are added to the Applicable System column for Part 3.1–3.5 it should also be included in Part 2.1-2.3. The process to authorize based on need except for CIP Exceptional Circustasnces would also algin.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	

Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Please clarify if EAMS and PAMS are to be treated as an applicable system subject device-type requirements (e.g. ports, patching, etc.) or if EAMS and PAMS are to be treated similar to BCSI, which appears to be the case. If they are intended to be treated similar to BCSI, they should not be included in the applicable systems column. They should only be in the requirements column. The periodic review requirements need to be clarified based on the intent. As written, quarterly review of BCSI-like repositories are required. As are two different types of access reviews every 15 months. This seems duplicative and inappropriate. The same issues are present with the access revocation tasks under Requirement R5.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
The exception should be for prior to granting authorized electronic access and authorized unescorted physical access to align with R2.2 training and Part 4.1 process to authorize based on need. Additionlly, if PCS are added to the Applicable System column for Part 3.1 – 3.5 it should also be included in Part 2.1-2.3. The process to authorize based on need except for CIP Exceptional Circustasnces would also algin.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	

We still have concerns about the splitting of EACMS and PACS into two different types. As mentioned before, has the drafting team considered when a device performs both functions what role it will have?   We agree with the modifications related to CIP Exceptional Circumstances. For CIP-004 R5.3, it is unclear why EAMS and PAMS are called out in the requirement when they are also in the applicability column. A BCS by its very nature has BCSI on it. EACMS and PACS (classical definition) may also have BCSI on it. If the SDT still believes that EAM and PAMS need to be called out in the requirement, then we recommend the following modification: "designated storage locations, including EAMS and PAMS, for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end..." Furthermore, CIP-004 R5.3 continues to be broken because technically it only applies to the applicable systems. There is not such concept as a BES Cyber System Information Repository, or storage, either physical or electronic, that contains BES Cyber System Information. All of CIP-011 also only applies to applicable systems. While most companies are applying BCSI protections to those items not listed in the applicable systems, technically they do not have to. However, this appears to be outside the SAR for this effort.

Likes 0	
Dislikes 0	

Response

Nathaniel Clague - Portland General Electric Co. - 1,3,5,6

Answer	No
Document Name	

Comment

PGE agrees with the changes related to CIP Exceptional Circumstances and PCS, but does not agree with the changes for EAMS and EACS. PGE supports BPA's comments related to lack of the desired outcome of allowing 3rd parties to perform roles on EACS and EAMS in the proposed applicability tables.

Likes 0	
Dislikes 0	

Response

12. The SDT is proposing modifications to CIP-005 (see the CIP-005 Technical Rationale document for detailed information). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The replacement of the ESP concept with Logical Isolation Zone (LIZ).

b. Is the backward compatibility clear as existing ESPs and EAPs move to the new LIZ concept?

c. The addition of the 4.2.3.3 exemption in the standard along with the addition of Requirement part R1.2 to address the V5TAG concern of "Super ESPs" or single networks within or between BES Cyber Systems that span more than one geographic location.

d. As differing forms of shared infrastructure come into play with virtualization, Requirement R3 has been added to include the management plane and its isolation controls as a part of the CIP standards. Is this concept clearly and widely understood?

Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

I beleive item "a" for LIZ will need more examples to help entities better understand how it can be identified and then documented to help ease any audit concerns.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	Yes
Document Name	

Comment

CIP-005 needs to be renamed. In general, we support the SDTs new definitions and terminology retirements. However, the structure of CIP-005 R1 requires mitigating risk of unauthorized communications, this seems to imply a requirement to authorize communication. Compliance with the new R1 and auditing could be problematic.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	
Comment	
CIP-005 needs to be renamed.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the replacement of the ESP concept with Logical Isolation Zone (LIZ). SRP does not agree the modifications are backwards compatible due to the expansion of applicability for various requirements. SRP agrees with the addition of 4.2.3.3 and the addition of R1.2 to clarify Cyber System geographic spans. SRP would like to see geographic spans more clearly defined as this may imply encryption between our primary and backup control centers. SRP also agrees with the comments from APPA.	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
The concept is clear but is not widely understood. A learning curve is to be expected.	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The concept is understood by people famiar with computing concepts.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Requirement part R1.2 appears to imply end-to-end encryption as the security objective. We recommend further clarification between CIP-005 R1.2 and CIP-012 to solidify the intent.	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP recommends the diagrams from the webinar be included in the technical rationale to more clearly illustrate how the concepts of Logical Isolation Zones would be applied to new and virtualization technology.	
Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Regarding c: Encryption should be in place between the two end-points shown in the diagram. Also, the same level of firewall controls should be enabled within both environments. However, there really doesn't seem to be a logical alternative to encryption to allow for disparate LIZs. Regarding d: The management planes should reside in completely isolated layer 3 networks that are not accessible by other workloads or layer stacks from the other LIZs and/or mixed mode environments. VLANS and VXLANS should not be used to isolate the management planes. Additionally, multi-factor authentication should be used along with separate authentication domains. These management planes, if compromised, would provide the “keys to the kingdom.”	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Backwards compatibility seems to be there, but it will require a review of all current network diagrams to see if all of our ESPs can be LIZs or if we want to consolidate/regroup certain systems into a LIZ. R1.2 addresses the fact that LIZ can be in different geographical locations. R3 is not clearly understood.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	

Backwards compatibility seems to be there, but it will require a review of all current network diagrams to see if all of our ESPs can be LIZs or if we want to consolidate/regroup certain systems into a LIZ. R1.2 addresses the fact that LIZ can be in different geographical locations. R3 is not clearly understood.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Seattle City Light contributed to and supports the comments provided by APPA.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	

Comment

Button response should be "No". Button selection wasn't allowed.

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

The SDT did a good job here.

{C}a) Comments above in #6 cover the LIZ

{C}b) Yes

{C}c) PAC appreciates the exception language related to the implementation of the super ESP.

{C}d) In CIP-005-7 the SDT capitalized the two terms Management Plane and Data Plane. Was this intentional? PAC understands the concepts presented.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

a. Texas RE does not agree the ESP concept should be replaced with Logical Isolation Zone (LIZ), since LIZ currently can exist within the current ESP concept. Please see Texas RE's response to #6.

b. Registered Entities may or may not be "backward compatible" with the LIZ concept. The LIZ concept would require network zoning, where ESP concept currently does not. If registered entities do not having network zoning, they would not be backward compatible. Texas RE notes that the LIZ concept can currently be done within the ESP concept.

c. Texas RE maintains ESP and EAP do nit need to change, so the exemption in CIP-005 Part 4.2.3.3 exemption is not needed.

Texas RE agrees with CIP-005 Part 1.2 but it should say "Protect the data traversing communication networks used to provide connectivity between **ESPs** that spans multiple geographic locations to preserve confidentiality and integrity."

c. Texas RE agrees with CIP-005 Part 3.1 and acknowledges that it does address virtualization. Texas RE recommends the following in the Applicable Systems column:

- EACS and PCS should be replaced with EACMS and PCA
- There appears to be a typo: "*Medium Impact BES Cyber Systems and their associated* ***PCS***"; "PCS" should be removed.

Likes 0

Dislikes 0

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer

Document Name

Comment

Cowlitz agrees with APPA comment.

Likes 0

Dislikes 0

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3

Answer

Document Name

Comment

While Virtualization needs to be addressed, additional implementation guidance is needed on "how" to treat virtualization, especially the isolation of BES vs. non-BES Cyber Assets on the same virtual infrastructure. Most entities have been separating the two; however, this separation is more costly.

Likes 0

Dislikes 0

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer

Document Name

Comment

The virtualization changes that are proposed will likely permit some mixed trust applications but it isn’t yet clear how logical isolation zones will provide better or equivalent protections to that of an ESP.

12.c. MRO supports the concept of a “Super ESP” that leverages encryption or equivalent logical protections initiated and terminated inside geographically separated ESP locations. The Logical Isolation Zone described in the 4.2.3.3 exemption however is not yet understood to be an equivalent or superior security protection.

Likes 0

Dislikes 0

Response

Jack Cashin - American Public Power Association - 4

Answer

Document Name

Comment

a. APPA agrees with the replacement of the ESP concept with Logical Isolation Zone (LIZ). Still better might be the overlay approach, in which both ESP and LIZ are options for an entity. Under such an option the existing definitions of EACMS and ERC might need to be updated to include “…Electronic Security Perimeter or Local Isolation Zone…” (i.e., add LIZ concept) to allow appropriate flexibility.

b. No. See discussion under Question 6.

c. Unclear. There is also concern that new approach to “Super-ESPs” is not backwards compatible as regards to communications among serially-connected BCS without ERC, and for relay tele-protection systems. For serial connected BCS, the new approach appears to expand the scope and treat communications for these cases the same as if there was ERC, which is not the way such cases are audited now. At present, a communication “demarcation” is identified for the non-ERC BCS at each end, and communications outside this demarcation are exempted, and no encryption or other security is required. For relay tele-protection, it appears to extend the BCS to include both ends, thereby raising to Medium any otherwise Low-impact rated substation connected by tele-protection to a Medium rated substation. Again, this expands the scope. In general, as a guiding principle, any expansion of scope to accommodate new vulnerabilities introduced by virtualization should be limited in applicability only to virtualized BCS.

d. Public power generally agrees with the addition of 4.3.3.3 and the addition of R1.2 to clarify Cyber System geographic spans. However, these additions do have several aspects that raise questions. For example, Requirement R3 regarding management plane concept will require implementation to understand the implications. Will there be a need to “future proof” the language related to the R1 exclusion? How will registered entities document the exclusion of time-sensitive protection or control functions?

Likes 0

Dislikes 0

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
a. Agree, although it creates a documentation burden. b. Yes c. How are entities to document exemptions? d. How will the removal of the term ERC affect serially connected substations where no remote access capability exists?	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
(a) LIZ may be better understood once additional clarity on logical security zone is provided. (b) Backward compatability is dependent upon previous questions asked and their results. (c) Yes (d) We believe there are too many dependencies at this stage to determine “clear and understood” status. CIP-005-7 R1.2: Duke Energy requests clarification on the differences between, or how R1.2 interrelates with CIP-006-7 R1.10. On its face, these two appear to be redundant. Additional language distinguishing one from the other, or perhaps Implementation Guidance on these would be helpful. CIP-005-7 R3: Is it the SDT’s intent for proposed R3 to be more expansive than what is currently protected? Is the SDT intending to bring in for example, the management interface of a firewall for the EACS?	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	

MISO requests that the SDT:

Unify the terminology between LIZ and “Super-ESP”

Provide clarity on the encrypted/protected data requirement. In particular does this requirement only apply if the data is leaving a PSP and is out in public spaces between the separate parts of the “Super-ESP?” If the requirement applies even when the data is still within a PSP that may require significant network complexity for minimal risk avoidance.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

While we do not have specific comments on questions a-b, we do have a comment on questions c and d and some concerns about certain updates within CIP-005.

c. We would like for the SDT to provide some examples within IG of how ESP would meet the definition of LIZ. We do have some concerns that auditors will need to have additional training to be able to audit the new LIZ.

d. We agree that in a mixed-mode virtual environment, isolation between the management plane and data plane becomes imperative (with mixed-mode meaning, for example, high/medium BES Cyber Systems, BES Cyber Systems/EACS, or CIP/non-CIP). However, if an entity sets up separate virtual environments (i.e. a high impact BES Cyber System virtual environment and a separate associated High Impact EACS environment) we believe that isolation between the management plane and the data plane will require a significant amount of extra work that will result in elevated compliance risk and zero benefit. The SDT should continue to consider that not all virtual environments that involve CIP will be mixed-mode. It should be clear in the requirements that if you protect the management plane as a part of the BES Cyber Systems the isloations requirements of Part 3.1 become nothing more than an exercise for compliance.

Other Comments:

Part 1.4 lists PCS as an applicable system and refers back to groupings under 1.1. However, Part 1.1 does not include PCS. Was this intentional by the SDT? To be consistent, we believe that PCS need to be added to 1.1 or removed from 1.4.

Additionally, the Secure Configuration concept is found throughout CIP-005. Please see our comment relating to Secure Configuration under question 15.

Finally, can the SDT provide information on the difference between CIP-005 R1.2 and CIP-006 R1.10? Under CIP-006 you can use physical protections and/or encryption to protect data that runs between LIZ, this seems to be duplicated under the new requirement of CIP-005 R1.2. We realize that CIP-005 talks about protecting data and CIP-006 discusses the physical protection of the cable, but both requirements are completeing basically the same function. This could result in double jeapory.

Likes 0	

Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy does not support all the changes being considered by the SDT for CIP-005 because we do not agree that the CIP Standards should be upended in order to accommodate a very small number of virtualized systems currently operated or being considered.

NV Energy does support the revisions to R1.2 for a “Super ESP”. As an Entity that currently deploys this type of ESP, the inclusion of defining this ESP would improve the existing Auditing practices for this type of system.

NV Energy also asks the SDT to consider the broad impacts and risk that the proposed wholescale replacement of the existing defined terms will have on Responsible Entities, who have worked to ensure the security of their BES Cyber Systems through the currently approved requirements. While we do not dispute that over time “zone” type security will replace the current “perimeter” type solutions, we disagree that this is the right time for such broad and sweeping changes. Instead, the SDT should take a less aggressive posture toward virtualization and narrow this effort to less complicated steps that might assist Responsible Entities in their efforts to virtualize portions of their BES Cyber Systems. Moreover, working within the current CIP structure will allow Responsible Entities to take smaller, less risky steps that will also reduce security and compliance issues for the industry.

Additionally, while the SDT proceeds with this effort, we respectfully ask them to consider providing more time for the industry to review, analyze, and determine where there might be issues related to proposed solutions to virtualization in order to ensure SMEs can thoughtfully assess, with greater confidence, that the proposed solutions will not create unintended disruptions while ensuring backward compatibility with existing BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

Do the proposed changes intend to include the EACS inside or outside the LIZ?

The concept of LIZ is not perimeter based and so it is not clear what or where an EACS is. Previous language was more clear that it was an Access Point, Intermediate System, or internal authentication system (e.g. LDAP inside the ESP).

In the proposed EACS concept, does a host-based firewall count as an EACS? Does a switch with an ACL count as an EACS? Does a network firewall inside an ESP implementing segmentation count as an EACS? Does a system's authorized users and authentication config count as its own EACS? Entities may define, in compliance with CIP-005-7 RequirementR1.1, their EACS protecting their BCS. However, there is compliance risk with the entities' choices because EACS is not well defined as being external to BCS/PCS in the LIZ or at the LIZ perimeter.

Additionally, access to a system using serial connection is allowed in CIP-005-7 Requirement R1.1, but not addressed much elsewhere. Is the intent that requirements for user restriction on IRA, encryption of connection to an intermediate system, and multi-factor authentication at an intermediate system apply to serial connections? This is unclear in the proposed standard.

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	

Comment

CHPD is concerned about the overlap of CIP-005 R1 Part 1.2 and CIP-006 R1 Part 1.10. The protection of so-called "Super ESPs" seems to already be covered by the CIP-006 R1 Part 1.10. Only one of the requirements should be maintained, and given that CIP-006 R1 Part 1.10 is already in effect, it is CHPD's preference that it be maintained over CIP-005 R1 Part 1.2.

CHPD also has concerns about the ambiguity of the management plane. Many devices do not have dedicated management planes, such as a server with remote desktop enabled. While it is best practice to separate your management plane from your data plane, many devices either would not support that or their function would be greatly degraded by having to disable management capability that cannot be isolated. Additionally, this requirement would apply to EACS, bringing network connectivity requirements to a classification of assets that did not before have connectivity requirements.

The concept of the LIZ does not seem to work if CIP-005 R3 is not considered. Depending on the interpretation of what a management plane is, significant rework of the network may be needed to separate it from the data plane. Take, for example, a PC-based system that is managed using remote management software (RDP, SSH, VNC, etc…). These systems and protocols could easily be considered to be "management plane" without any specific definition or language to say otherwise. The problem with this is that there is no feasible method for separating these kinds of PC-based management services from the "data plane" like can be easily done for a switch, firewall or hypervisor. The current scope of R3 includes BCA, EACS and PCS, so Windows and other similar PC-based Cyber Assets would definitely fall under the requirement, as written. Without a definition for "management plane" that properly scopes devices that do support separation of a management plane (e.g., switches, firewalls, routers, hypervisors, etc…) there is little likelihood that any existing Medium of High Impact-owning entity could establish a method for achieving compliance with this language. One recommendation for fixing this problem is to specifically identify those system types, either by definition or within R3 itself, that require management plane separation.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No
Document Name	
Comment	
Introduction of a new term logical isolation zone rather than ESP introduces confusion in the definition and with backward compatibility. For example, the definition would now be applicable to serial communications. This is an example of a definition that will be debated for several years in the industry. Continue with our current industry standard definition or ESP and adjust the standards language to address issues or adopt standard NIST terms. SuperESPs can be accommodated by changes to requirements rather than definitions as the current definition of an ESP does not prevent multi-site ESPs.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 12.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
Exelon does not support the changes being considered by the SDT for CIP-005 because we do not agree that the CIP Standards should undergo this level of significant change for the purpose of accommodating the needs of a relatively small number of mixed virtual environments currently operated or being considered. The proposed change to move from a layer 3 "perimeter" to a "logical isolation zone" philosophy introduces a significant learning curve. There may be serious risks to security through misunderstandings of vulnerabilities and how to properly implement, by both Responsible Entities and auditors. Exelon also asks the SDT to consider the broad impacts and risk that the proposed wholescale replacement of the existing defined terms will have on Responsible Entities, who have worked to ensure the security of their BES Cyber Systems through the currently approved requirements. While we do not dispute that over time "zone" type security will replace the current "perimeter" type solutions, we disagree that this is the right time for such broad and sweeping changes. Instead, the SDT should take a less aggressive posture toward virtualization and narrow this effort to less complicated steps	

that might assist Responsible Entities in their efforts to virtualize portions of their BES Cyber Systems. Moreover, working within the current CIP structure will allow Responsible Entities to take smaller, less risky steps that will also reduce security and compliance issues for the industry.

Additionally, while the SDT proceeds with this effort, we respectfully ask them to consider providing more time during the standard development process for the industry to review, analyze, and determine where there might be issues related to proposed solutions to virtualization in order to ensure SMEs can thoughtfully assess, with greater confidence, that the proposed solutions will not create unintended disruptions while ensuring backward compatibility with existing BES Cyber Systems.

Likes 0

Dislikes 0

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0

Dislikes 0

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	No
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"EEI does not support the changes being considered by the SDT for CIP-005 because we do not agree that the CIP Standards should be upended in order to accommodate a very small number of virtualized systems currently operated or being considered. Additionally, changes such as moving from a “perimeter” to a “zone” philosophy may result in serious risks to security through misunderstandings of what exactly that means by both Responsible Entities and auditors, which is not currently justified.

EEI also asks the SDT to consider the broad impacts and risk that the proposed wholescale replacement of the existing defined terms will have on Responsible Entities, who have worked to ensure the security of their BES Cyber Systems through the currently approved requirements. While we do not dispute that over time “zone” type security will replace the current “perimeter” type solutions, we disagree that this is the right time for such broad and sweeping changes. Instead, the SDT should take a less aggressive posture toward virtualization and narrow this effort to less complicated steps that might assist Responsible Entities in their efforts to virtualize portions of their BES Cyber Systems. Moreover, working within the current CIP structure will allow Responsible Entities to take smaller, less risky steps that will also reduce security and compliance issues for the industry.

Additionally, while the SDT proceeds with this effort, we respectfully ask them to consider providing more time for the industry to review, analyze, and determine where there might be issues related to proposed solutions to virtualization in order to ensure SMEs can thoughtfully assess, with greater confidence, that the proposed solutions will not create unintended disruptions while ensuring backward compatibility with existing BES Cyber Systems."

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

The note should not be used within requirement language in Part 1.1 and other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location.

Geographic location should be clarified on Part 1.2. It is unclear how this would apply to multiple buildings within a single campus. These buildings may have different PSPs while in the same campus.

For Part 1.4, consider using “per system capability” instead of “excluding serial port connectivity such as RS-232 and RS-485”.

For Part 2.2, consider the following, “Have one or more methods at the point of termination to mitigate the risks posed by unauthorized modification and unauthorized disclosure of data during all Interactive Remote Access sessions.”

For Part 2.3 consider the following, “Have one or more methods of multi-factor authentication for all Interactive Remote Access sessions.”

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Although N&ST is supportive of the general concept of replacing the network-centric definition of “ESP” with a more flexible, “secure enclave” concept, we have a number of concerns:

>> N&ST believes the current proposed definition of “LIZ” needs to be clarified. Suggested re-wording: “A logical container, or enclave, that encloses one or more BES Cyber Systems and applies a common set of controls to all communications to or from those BES Cyber Systems.”

>> N&ST believes the desired “backward compatibility” needs to be made more clear. N&ST suggestions include (1) revising the definition of “LIZ,” as per above, (2) adding explicit language to R1 to the effect that applicable systems must be located with a “LIZ,” and (3) Cyber Asset(s) used to provide the necessary control of communications into and out of a “LIZ” must, if not already part of an applicable system, be identified as EACMS or EACS.

>> N&ST opposes the proposal to exempt Cyber Assets within a “LIZ” if they are associated with communications links between multiple geographic locations. N&ST believes such an exemption carries the risk of creating “soft spots” within logical boundaries that are supposed to be highly secure.

>> N&ST believes the concept of isolating the management and data planes of virtual systems is reasonably well understood, but we are concerned about the fact there are no further requirement statements about the management plane in any of the modified Standards. N&ST believes that at a minimum, the management plane(s) of virtual systems (e.g., Hypervisor) should be categorized as EACMS or EACS.

>> N&ST has an additional concern about the proposed changes to CIP-005: As written, R1 could, N&ST believes, be interpreted as applying to ALL high and medium impact BES Cyber Systems, regardless of whether or not they communicate using routable protocols.

Likes 0	
Dislikes 0	

Response

Lana Smith - San Miguel Electric Cooperative, Inc. - 5

Answer	No
Document Name	

Comment

SMEC disagrees with ESP replacement. It will require additional documentation, especially for serial connected devices. LIZ should only apply to the virtual devices.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6

Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST.

In addition, how is the proposed CIP-005 R1.2 different from CIP-006 R1.10? Seems there is overlap as it relates to encryption of data.

Also, SDT needs to explain the comment “Examples include physical protections and points where encryption initiates and terminates.” Is this suggesting physical protection must be applied to encryption points, or that this requiring both physical measures and encryption?

Need to better define communication networks. Which protocols are in scope vs. out of scope, and how are third-party networks treated?

Regarding CIP-005 R1.4, SDT needs to provide guidance / clarity on the term “privileged introspection.”

And generally speaking, needs to clarify the use of system or asset throughout the standards, as the current proposed revisions do not seem to be consistent, and using undefined terms will make it difficult to establish device applicability.

Regarding the Virtual Machine concept, the entire Virtual Machine / system, including the hypervisor, must be part of the BCS with CIP controls applied. If someone can comprise the hypervisor and disable or compromise the virtual machines / systems (BCS) that could have 15-minute impact, it should also be a BCS. High-water mark everything or require segmentation.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO

Answer	No
Document Name	

Comment

Please see MRO NERC Standards Review Forum (NSRF) comments.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5

Answer	No
Document Name	

Comment

PSE supports the comments developed by EEI.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	
Comment	
Support MRO NSRF comments	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
As stated in #6 LCRA has concerns about the implementation of the LIZ definition in its current form.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
a. Agreed with the following caveat; the proposed definition of LIZ needs to be re-evaluated and clarified. b., c., d. The proposed definitions need to be re-evaluated and clarified before additional meaning full comments can be considered.	
Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No

Document Name	

Comment

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry’s programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

-

    No. We do not think ESP needs to be changed.

    No. We think it will require additional documentation, especially for serial connected devices.

    Yes.

No. We question how this applies to technology such as the Dell DRAC or large network backplane systems.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	AZPS Comments - Question 12.docx

Comment

Please see the attached document.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

a. Agree

b. Agree

c. Agree

d. We understand the concept of isolation between the management plane and the data plane, however there was no discussion or explanation of the CIP controls that may be required for the management plane (aka Central Management Servers ?)

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

More education is needed before implementing such changes. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	No
Document Name	

Comment

Changing from ESP to LIZ is unclear and requires a change in the fundamental understanding to the cyber security that is in place today

Also a scope change because Medium Impact had two variations. For certain Requirements, BES Cyber Assets had exceptions when there was no External Routable Connectivity

Part D we do not believe that the concept of isolated and control of the management plane is widely understood.

We do not support the changes being considered by the SDT for CIP-005 because we do not agree that the CIP Standards should be upended in order to accommodate a very small number of virtualized systems currently operated or being considered. Additionally, changes such as moving from a “perimeter” to a “zone” philosophy may result in serious risks to security through misunderstandings of what exactly that means by both Responsible Entities and auditors, which is not currently justified. We also ask the SDT to consider the broad impacts and risk that the proposed wholescale replacement of the existing defined terms will have on Responsible Entities, who have worked to ensure the security of their BES Cyber Systems through the currently approved requirements. While we do not dispute that over time “zone” type security will replace the current “perimeter” type solutions, we disagree that this is the right time for such broad and sweeping changes. Instead, the SDT should take a less aggressive posture toward virtualization and narrow this effort to less complicated steps that might assist Responsible Entities in their efforts to virtualize portions of their BES Cyber Systems. Moreover, working within the current CIP structure will allow Responsible Entities to take smaller, less risky steps that will also reduce security and compliance issues for the industry. Additionally, while the SDT proceeds with this effort, we respectfully ask them to consider providing more time for the industry to review, analyze, and determine where there might be issues related to proposed solutions to virtualization in order to ensure SMEs can thoughtfully assess, with greater confidence, that the proposed solutions will not create unintended disruptions while ensuring backward compatibility with existing BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	No
Document Name	
Comment	
It appears that the intent of modification to CIP-005 R1.1 was to shift from an isolated ESP to an isolated LIZ. However, as drafted, it appears that this modification either (a) raises the burden by requiring firewalls on every BCS, or (b) uses the “system or group” term to refer to an LIZ. The language “applicable systems, either individually or as a group,” should be replaced with the term “LIZ.” The term “communication” could be augmented with “and access to internals and shared resources,” which would imply not only routable communication but also other mechanisms that could affect an LIZ. The proposed CIP-005 R1.2 may be redundant with CIP-006 R1.10. CIP-005 R3 needs additional clarification under “Applicable Systems” in order to be backward-compatible. It may need a new class of asset such as “Zone Boundary System” to apply to. The intent of the Requirement appears to be to prevent an attacker from breaking LIZ boundaries. Most BCS, when they do have a management plane, do not have a management plane that can be used to break an LIZ boundary. If all aspects of a BCS, including management plane and internal virtualized Cyber Assets, are contained entirely within the same LIZ, then no change to its topology can break out of the LIZ. Only an asset that contains some part of an LIZ, but that has some presence in a zone external to the LIZ, could be used to gain unauthorized entry. That would be a Zone Boundary System. An example would be a hypervisor that contains a virtual switch with BCS on it. Access to the management plane of a Zone Boundary System could be used maliciously to reconfigure the virtual isolation and connect those BCS to external systems. Therefore, the proposed R3.1 should apply to Zone Boundary Systems associated with a Medium-Impact LIZ. The management plane should be considered a PCA at the “high water mark” rating of the LIZs contained within and should itself be entirely contained within a LIZ.	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

a. No. Reclamation does not support replacing ESP with Logical Isolation Zone (LIZ) as stated in the response to question 6. Reclamation recommends the SDT use the term Enclave to meet FERC's intent.

If new terminology is needed, Reclamation recommends using existing definitions from the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms (NISTIR 7298), specifically the NIST-defined terms "Enclave" and "Enclave Boundary."

Reclamation also recommends replacing the proposed Logical Isolation Zone (LIZ) term with the following term and adding it to the NERC Glossary of Terms:

Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

b. No. Reclamation does not support the term LIZ and recommends the SDT adopt the term ESE as described above and in the response to question 6. The proposed LIZ definition seems to combine the ESP and EAP concepts but is not as well defined as the individual ESP and EAP definitions.

Logical isolation must distinguish between BES and non-BES. A Logical Isolation Zone could become a risk to BES Cyber Systems when stretched to corporate business enclaves through virtual machine hyper jumping from a lower trust business network. Mixed trust environments on common hardware between CIP Applicable Systems and corporate business networks could introduce risk to the BES.

c. No. As it is written, exemption 4.2.3.3 does not distinguish between entity-owned Cyber Assets and third party-owned Cyber Assets. Reclamation recommends the SDT clearly state the scope of the exemption.

Reclamation also recommends that Cyber Assets associated with communication networks and data communication links used to extend an Electronic Security Enclave to more than one geographic location be protected.

d. No. Requirement R3 seems to apply to Virtual Machines, but it is unclear what the "management plane" and "data plane" are relative to the Applicable Systems. Reclamation recommends the SDT align Requirement R3 to be backwards compatible with current configurations, or state that R3 specifically applies to Virtual Machine technology. Reclamation also recommends if the SDT does use the terms "Management Plane" and "Data Plane" in the standard, they should be defined in the NERC Glossary of Terms.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

We disagree with these changes. For the bullet a & b, we have the same comments as the above question 6. For the bullet c, the communication components between ESP at Control Centres has been addressed in CIP-006-6 R1.10, if SDT wants to protect the communication components between ESPs outside the Control Centres, SDT only needs to develop an additional requirement in CIP-006-6 to address that. For the bullet d, given that the current CIP V5 requirements have addressed the management plane implicitly, where the management plane devices must have been identified as EACMS since they can add, delete or modify CIP VMs and entire infrastructures. In our virtual environment, the management plane devices were identified as Intermediate Systems and fully compliant by the existing requirements.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

We do not think ESP needs to be changed.

a. No. The NSRF believes ESP replacement will require additional documentation, especially for serial connected devices.

b. No. The NSRF does not recommend replacing ESP with Logical Isolation Zone (LIZ).

c. No. The NSRF questions how this applies to technology such as the Dell DRAC or large network backplane systems.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro

Answer	No
Document Name	

Comment

BC Hydro agrees with the changes outlined under points 12a, 12b and 12c. However, on Question 12d additional clarification is needed, as it seems unclear what aspects of a system, and its functions and types of access (e.g. system to system or user remote access) would be considered part of the management or the data plane in both virtual and physical environments.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

The replacement of ESP to LIZ is appealing, but its ramifications have yet to be fully understood. While an existing ESP/EAP model may be able to port to the LIZ, the problem is the drafted changes have introduced other LIZ that may need to be implemented to be compliant with regard to serial communications and management planes. Per previous comments, we are still concerned about the issue of nesting LIZ and Entities being penalized for defense in depth when a single control fails, yet all other controls were still protecting the applicable systems.

The concept of “span more than one geographic location” gives us pause. The issue is what defines a geographic location. Per https://sciencing.com/geographic-location-mean-8667.html, a “Geographic location refers to a position on the Earth. Your absolute geographic location is defined by two coordinates, longitude and latitude.” The issue is what is the difference in longitude and latitude that constitute one geographic location be separate from another? Longitude can vary depending on the latitude that it is measured at. So just looking at latitude, one degree of latitude can span about 69 miles, a minute of latitude can span about 1.15 mi, and a second of latitude can span about 101 feet. So technically if you have a big enough campus with an A and B datacenter at the campus then you could have a network spanning more than one geographic location when measured down to the second of latitude and longitude. We applaud the SDT for actually trying to tackle a V5TAG issue since this has not been done for the issues of “Clarify the intent of ‘programmable’ in Cyber Asset”, “Clarify and focus the definition of ‘BES Cyber Asset’” and its three sub concerns, the issue of "associated" in the ERC definition, the concept of “directly” within the ERC definition, and the issue of IRA definition with “using a routable protocol” and the Guidelines and Technical Basis contradiction of dial-up connectivity for IRA means that R2 also applies. These are all the items in the SAR not addressed by the SDT in this proposed draft.

The concept of requiring a LIZ for the management plane is not clearly understood. Some devices may inherently come with a separate management plane interface like baseboard management controller on a server (e.g. HP iLO, DELL iDRAC, Cisco CIMC). However, many do not. Servers acting as a hypervisor have Network Interface Cards (NIC) assigned to various functions. Best practice would have a split of the data plane, management plane, storage plane, and motion or migration plane. However, the data plane and management plane can be on the same set of NICs and separated by VLANs. Since this separation is a design choice and not an inherent property, then does that mean all other machines including workstations must be outfitted with a set of management plan NICs per device capability and thus dual-homing all machines to both the management and data plan? While we appreciate the SDT trying to avoid overly prescriptive requirements, the current draft regarding data plane and management plane remains vague and open to varying interpretations of what compliance looks like.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

NRG does not agree with the replacement of the ESP concept with Logical Isolation Zone (LIZ) because serial ports and potentially 4-20mA inputs would be included under EAC or EAPs. Therefore, it would be difficult for registered entities' NERC CIP subject matter experts to understand and potentially difficult to implement as it would take significant resources for registered entities to revamp their entire NERC CIP compliance programs to accommodate these changes, which could affect their existing reliability or security postures. These proposed changes include fundamental changes to NERC CIP ESP and BCS concepts.

No, NRG does not assert that backward compatibility is clear as existing ESPs and EAPs move to the new LIZ concept, because it is not technically explicit and not explicit in its technical definition (no clear logical boundaries "in or out" due to retired key terms that help to build the framework of an ESP boundary).   This could cause reduced security and less ability to achieve compliance because it requires registered entities to take a more interpretive stance on achieving compliance as the proposed language is less prescriptive.

No, NRG does not agree that the addition of the 4.2.3.3 exemption in the standard along with the addition of Requirement part R1.2 to address the V5TAG concern of "Super ESPs" or single networks within or between BES Cyber Systems that span more than one geographic location, because NRG takes the 4.2.3.3 exemption to relate to VLANS. Attackers could manipulate network gear in-between EACs to compromise VLAN security.

No, NRG does not agree that as differing forms of shared infrastructure come into play with virtualization, Requirement R3 has been added to include the management plane and its isolation controls as a part of the CIP standards concept is clearly and widely understood. Registered entities would likely need to form additional understanding of these concepts with their vendors which may be broader than the intent of the proposed standard change.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

The note should not be used within requirement language in Part 1.1, or in other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location.

Geographic location should be clarified on Part 1.2. It is unclear how this would apply to multiple buildings within a single campus. These buildings may have different PSPs while in the same campus.

For Part 1.4, consider using "per system capability" instead of "excluding serial port connectivity such as RS-232 and RS-485."

For Part 2.2, consider the following, "Have one or more methods at the point of termination to mitigate the risks posed by unauthorized modification and unauthorized disclosure of data during all Interactive Remote Access sessions."

For Part 2.3 consider the following, "Have one or more methods of multi-factor authentication for all Interactive Remote Access sessions."

Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The EEI members who participated in the development of these comments do not support the changes being considered by the SDT for CIP-005 because they do not agree that the CIP Standards should be upended in order to accommodate a small number of virtualized systems currently operated or being considered. Additionally, there is concern that changes such as moving from a "perimeter" to a "zone" philosophy may introduce security risk due to misunderstandings or disagreement on these terms by both Responsible Entities and auditors. EEI recommends that the SDT consider the broad impacts and risks that the proposed wholesale replacement of the existing defined terms will have on Responsible Entities, who have worked to ensure the security of their BES Cyber Systems through the currently approved requirements. While there is no dispute that, over time, "zone" type security may replace the current "perimeter" type solutions, now may not be the right time for such broad and sweeping changes. Instead, we recommend that the SDT consider a less aggressive posture and narrow this effort to focus on targeted efforts to assist Responsible Entities in their efforts to virtualize portions of their BES Cyber Systems. Moreover, working within the current CIP structure will allow Responsible Entities to take smaller, less risky actions toward virtualization that will reduce the potential for security and compliance issues as the industry matures toward virtualized systems. Additionally, as the SDT proceeds with this effort, EEI respectfully requests that they consider providing more time for the industry to review, analyze, and determine where there might be issues related to proposed solutions to virtualization in order to ensure SMEs can thoughtfully assess, with greater confidence, that the proposed solutions will not create unintended disruptions while ensuring backward compatibility with existing BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
a: The concept of the LIZ allows for the introduction of new technologies to fulfill the requirements which is good. However, with a wide variety of possible solutions to available to fulfill the requirements there could also be a wide variety of audit approaches/auditor preferences that could make audits more challenging. b: Yes, a traditional ESP/EAP design seems to fit into the LIZ concept as is. c: No issues with the 4.2.3.3 exemption or the “Super ESP” concept. d: No issues with requirement R3 either, it’s logical and prudent.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
For clarity, Tri-State recommends Part 1.1 R1.1.1 be changed from "and" to "or" to accommodate different configurations and allow flexibility. This should read "Communication that has documented inbound and outbound access permissions, including the reason for granting access; or" Serial port connectivity….	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

a. We do not agree with replacing the ESP concept with LIZ. Is it the intent of the SDT that existing ESPs simply convert to a LIZ, where virtual technology does not exist?

b. With all the additions, deletions, and revisions to so many terms and definitions it is not possible at this time to be sure of backwards compatibility.

c. Unclear

d. Also, in R3 Isolation of Management Plane and Data Plane, these terms are initially defined in footnotes, and then capitalized in M3, then lower case again in 3.1. These terms should be explicitly defined in the Glossary.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA

Answer	No
Document Name	

Comment

Changing from ESP to LIZ is unclear and requires a change in the fundamental understanding to the cyber security that is in place today

Also a scope change because Medium Impact had two variations. For certain Requirements, BES Cyber Assets had exceptions when there was no External Routable Connectivity

Part D we do not believe that the concept of isolated and control of the management plane is widely understood.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern supports the direction of CIP-005 and logical isolation of systems. We have concerns regarding R3 as it applies to all high and medium impact systems and not just those that utilize shared infrastructure. It is not clear exactly what the management plane and the data plane is on every high or medium impact system in existence. The data plane for instance is defined as "part of the network that carries user traffic" per the footnote. It is not clear how an entity on a firmware-based system with one network port will isolate the management plane from "the part of the network that carries user traffic." We also believe R1.2 is not scoped correctly. The language scopes it to all data on any network (LAN or WAN) within the "components of a LIZ" if that LIZ happens to span geographic locations. It needs to be scoped to just those networks used to span the different geographic locations and not all components within the LIZ, such as two hosts in the same cabinet. For R1, Southern is concerned over the "Secure Configuration" and its interaction with a "method" of isolation and change management in CIP-010. Devices such as LAN/RAN serial converters and Dynastars (i.e. mixed serial and IP configurations) and how to implement them need additional clarity. If a particular device cannot support encryption but the rest of the devices can, will I be able to reasonably scope my secure configuration at the device level for components, but also have a separate secure configuration for the "rest of the system"? R3 does not fit non-virtualized environments well.

Likes 0	
Dislikes 0	

Response

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0	
Dislikes 0	

Response

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

a. No. WAPA does not support replacing ESP with Logical Isolation Zone (LIZ) as stated in the response to question 6. WAPA strongly recommends the SDT use the term Enclave to meet FERC's intent.

WAPA recommends using existing definitions from the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms (NISTIR 7298), specifically the NIST-defined terms "Enclave" and "Enclave Boundary."

WAPA also recommends replacing the proposed Logical Isolation Zone (LIZ) term with the following term and adding it to the NERC Glossary of Terms:

Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

b. No. WAPA does not support the term LIZ and recommends the SDT adopt the term ESE as described above and in the response to question 6. The proposed LIZ definition seems to combine the ESP and EAP concepts but is not as well defined as the individual ESP and EAP definitions.

Logical isolation must distinguish between BES and non-BES. A Logical Isolation Zone could become a risk to BES Cyber Systems when stretched to corporate business enclaves through virtual machine hyper jumping from a lower trust business network. Mixed trust environments on common hardware between CIP Applicable Systems and corporate business networks could introduce risk to the BES.

c.	No. As it is written, exemption 4.2.3.3 does not distinguish between entity-owned Cyber Assets and third party-owned Cyber Assets. WAPA recommends the SDT clearly state the scope of the exemption.

WAPA also recommends that Cyber Assets associated with communication networks and data communication links used to extend an Electronic Security Enclave to more than one geographic location be protected.

No. Requirement R3 seems to apply to Virtual Machines, but it is unclear what the “management plane” and “data plane” are relative to the Applicable Systems. WAPA recommends the SDT align Requirement R3 to be backwards compatible with current configurations, or state that R3 specifically applies to Virtual Machine technology. WAPA also recommends if the SDT does use the terms “Management Plane” and “Data Plane” in the standard, they should be defined in the NERC Glossary of Terms..

Likes 0	
Dislikes 0	

Response

13. The SDT is proposing conforming modifications to CIP-006. Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. Modifications related to CIP Exceptional Circumstances

b. Use of newly proposed term EACS in the Applicable Systems column

Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
SMEC agrees with modifications related to CIP Exceptional Circumstances. SMEC believes further guidance should be provided to define the split of EACMS	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	
Answer	Yes
Document Name	
Comment	
b. The SDT has correctly identified that EACS and EAMS should not require the same CIP protections.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	

Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
If a system that controls access to a BES Cyber System (EACS) is compromised, the real-time ability to operate or control the BPS could be reduced or severed altogether. For this reason, we are in agreement with the use of the newly proposed term EACS throughout CIP-006. Additionally, the modifications related to CIP Exceptional Circumstances bring continuity throughout. See comment in question 12 about CIP-006 R1.10.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
We support the changes related to the EACMS and PACS.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Recommend removing TFE from CIP-006 Part 1.3 similar to the removal of TFE from CIP-007.	

Recommend having a process to define a PACS asset, including required Identification and classification.

Recommend requiring a response process for the 15 min alarm.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

Add CIP Exceptional Certcumstances for CIP 006 R1.3 to allow for emergency personell to respond without a requirement of two factor authentication

Likes 0	
Dislikes 0	

Response

Joseph Pride - Trans Bay Cable LLC - 1 - WECC

Answer	Yes
Document Name	

Comment

These changes appear reasonable. Changes to CIP Exceptional Circumstances relieve controls on authorized persons but remove such relief for visitors during CIP Exceptional Circumstances. Relieving controls on authorized persons is consistent with the concept that authorized people may need to act outside of the normal controls. However, authorizing or controlling visitors remains important. Corresponding reliefs under CIP-004 make it possible to grant new authorizations without the lead time of a PRA process, allowing (but still requiring) rational management of emergency staff augments such as incident management consultants during CIP Exceptional Circumstances.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	
Comment	
a) no comment b) no comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the update to include EACS in place of EACMS. SRP also agrees with adding the CIP Exceptional Circumstance exception to the requirements. Additionally, SRP agrees with the comments from APPA.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	

Answer	Yes
Document Name	
Comment	
Hydro One supports TFIST comments suggesting that PACS and PAMS should be subject to maintenance and testing per CIP-006, R3.1.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer

Document Name

Comment

Seattle City Light contributed to and supports the comments provided by APPA.

Likes 0

Dislikes 0

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer

Document Name

Comment

No comment.

Likes 0

Dislikes 0

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer

Document Name

Comment

Button response should be "No".   Button selection wasn't allowed.

PacifiCorp’s approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

The SDT did a good job here. PAC disagrees with EACMS and PACS changes and believe we can accomplish the same without the new terms.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

a. Public power agrees with the addition of the CIP to the requirement level for R2. It seems appropriate to maintain the CIP Exceptional Circumstances (CEC) for R1 related to access logs. However, we suggest NERC consider that alarm requirements in R1 could also be covered by CEC in the event of “an imminent or existing hardware, software, or equipment failure.”

b. APPA agrees with the change to use the EACS in the Applicable Systems column. We appreciate the fact that the EAMS are not included as we anticipate that they will be covered under other BCS-related standards. This provides another option to use the dual-definition approach and allow entities to select between either the existing EACM definition and requirements or use the new EAC/EAM definition and proposed new requirements.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	
Document Name	

Comment

abstain

Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	
Comment	
Cowlitz supports APPA comment.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
a. Texas RE does not have an issue with the SDT adding CIP Exceptional Circumstances for Parts 1.8, 1.9, or R2. b. Please see Texas RE's response to #4 regarding the EACMS definition.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
NYPA supports comments submitted by NPCC / TFIST.	

In addition, the SDT did not clearly demonstrate an added security benefit to these proposed changes that would justify the administrative burden and cost of implementation.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

Removal of the allowance for CIP Exceptional Circumstance for R2 Part 2.1 and R2 Part 2.0 is a mistake. In the event of a physical emergency (e.g. fire, active shooter, chemical spill, etc.) the use of an escort likely will not be allowed by emergency personnel.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST supports the modifications related to CIP Exceptional Circumstances but opposes the exclusion of systems that perform electronic or physical monitoring.

Likes 0	
Dislikes 0	

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	No
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI: "In general, comments made in response to Question 11 also apply to our concerns with CIP-006."	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
In general, comments made in response to Question 11 also apply to our concerns with CIP-006.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 13.	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
CHPD is concerned about the overlap of CIP-005 R1 Part 1.2 and CIP-006 R1 Part 1.10. The protection of so-called "Super ESPs" seems to already be covered by the CIP-006 R1 Part 1.10. Only one of the requirements should be maintained, and given that CIP-006 R1 Part 1.10 is already in effect, it is CHPD's preference that it be maintained over CIP-005 R1 Part 1.2.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
In general, comments made in response to Question 11 also apply to our concerns with CIP-006.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

a. No. During an extreme weather event a CEC may be declared. For instance, if a tornado hit a substation and compromised the control building a CEC would be required for all of R1 not just the Parts in the proposed change. We recommend leaving the CEC at the R1 level.

b. No. We think that EAMS should also be afforded the same protections as EACS. It is a generally accepted security concept that if a person has physical access to a system it is difficult to prevent them from compromising that system. EAMS are an important part of providing security for BES Cyber Systems and should thus be afforded the same physical protections.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

a. Yes. Reclamation agrees with the modifications related to CIP Exceptional Circumstances. CIP Exceptional Circumstances are necessary during emergencies for first responders.

b. Reclamation supports adding systems that control access to the Applicable Systems column; however, Reclamation disagrees with the newly-proposed term EACS. Reclamation recommends the SDT use the term Intrusion Detection System (IPS) instead, as stated in the response to Question 4.

Reclamation recommends CIP-006 Requirement R1 Part 1.10 be changed

from:

Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:…

to:

Where physical access restrictions to such cabling, components, or Cyber Assets associated with communication networks and data communication links cannot be implemented, the Responsible Entity shall document and implement the following:…

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC

Answer	No
Document Name	

Comment

The removal NERC CIP Exceptional Circumstance language at the requirement level seems to be in opposition of the stated intent of the stated use of NERC CIP Exceptional Circumstance.

Standard emergency procedures seem to be disallowed by the inclusion of CIP Exceptional Circumstances at the sub-Requirement level and not at the Requirement level

We suggest that PACS and PAMS should be subject maintenance and testing per R3.1

Likes 0

Dislikes 0

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

MEC does not agree with the conforming changes. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

Likes 0

Dislikes 0

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

a) No. During an extreme weather event a CEC may be declared. For instance, if a tornado hit a substation and compromised the control building a CEC would be required for all of R1 not just the Parts in the proposed change. We recommend leaving the CEC at the R1 level.

b) No. We think that EAMS should also be afforded the same protections as EACS. It is a generally accepted security concept that if a person has physical access to a system it is difficult to prevent them from compromising that system. EAMS are an important part of providing security for BES Cyber Systems and should thus be afforded the same physical protections

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

a. Agreed

b. The proposed definitions need to be re-evaluated and clarified before additional meaning full comments can be considered

Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Support MRO NSRF comments

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	No
Document Name	

Comment

Southern Company believes the CEC in CIP-006 R1.8 and R1.9, while helpful, only addresses logging failures. In a storm response mutual assistance situation, for example, you would still have to control, monitor, and alert on access, even if the entire PACS is lost, not just the logging function. With this situation, it seems that there are now less restrictions on visitors during a CEC in R2 than the employees who are on site repairing the system. Southern Company asserts that it will make more sense to move the CEC language to the higher level requirement level (R x) rather than the sub-requirement level (R x.y).

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group

Answer	No
Document Name	

Comment

a. During an extreme weather event a CIP Exceptional Circumstance ("CEC") may be declared. For instance, if a tornado hits a substation and compromised the control building a CEC would be required for all of R1 not just the Parts in the proposed change. We recommend leaving the CEC at the R1 level.

b. The SSRG believes that EAMS should also be afforded the same protections as EACS. It is a generally accepted security concept that if a person has physical access to a system it is difficult to prevent them from compromising that system. EAMS are an important part of providing security for BES Cyber Systems and should thus be afforded the same physical protections.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA

Answer	No
Document Name	

Comment

The removal NERC CIP Exceptional Circumstance language at the requirement level seems to be in opposition of the stated intent of the stated use of NERC CIP Exceptional Circumstance.

Standard emergency procedures seem to be disallowed by the inclusion of CIP Exceptional Circumstances at the sub-Requirement level and not at the Requirement level

We suggest that PACS and PAMS should be subject maintenance and testing per R3.1

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	No
Document Name	

Comment

a. Agree with the addition of CEC for the reqiuirement level of R2. Recommend it be maintain at the requirement level for R1. In the event of a catastrophic event an entitiy may have to declare a CIP Exceptional Circumstance that may require CEC all parts of R1.

b. If EACMS is split into EAMS and EACS, what would be considered an EAMS? The camera systems or software used to perform electronic monitoring? CIP-006 only requires Electronic Control Systems (EACS) and no Electronic Monitoring Systems (EAMS). So an entity has to control access but does not have to monitor it, was this the intent of the SDT?

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

In general, comments made in response to Question 11 also apply to our concerns with CIP-006.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No

Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
While we do not have any problem with the conforming modifications to CIP-006, we are still concerned about the other concepts that are driving the modifications as mentioned in our other comments.	
Likes 0	
Dislikes 0	
Response	

14. The SDT is proposing modifications to CIP-007 (see the CIP-007 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The SDT is proposing adding the security objectives throughout the Requirements in CIP-007. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?

b. The SDT is proposing the security objective in CIP-007 R1, “to mitigate the risk posed by uncontrolled logical and physical connectivity". Do you agree that the modifications to CIP-007 R1 Part 1.1 fulfill this security objective for systems where connectivity is not limited to TCP/IP port service combinations, as in virtualized systems and SAN based storage?

c. Do you agree that the modifications to CIP-007 R1 Part 1.1 add necessary flexibility to fulfill the security objective of CIP-007 R1 for virtualized systems and provides a degree of future proofing?

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

a) Yes, the additions help clarify intent. As with any compliance standard, it is important to integrate the intent with the method of auditing to allow the intent to be the focus and not prescriptive details. This also needs to be clearly and consistently communicated throughout the regions.

b) Yes.

c) Yes.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

CIP-007-7, Requirement R1, Part 1.2 regarding the protection of unused physical ports. The Secure Configuration is not present in this Requirement and I believe it should be. The potential protections can be physical or logical, and a change could impact either one of these. For logical, it is easy to understand a change could change the logical setting of a port making it usable. For a physical change, a similar condition could occur of the change was the swap out of hardware and a physical port blocker was not re-installed or signage is not put back into place.

Likes 0	

Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP does not agree or disagree that the proposed security objectives add clarity to the reason the requirement exists. SRP also agrees the modification to CIP-007 R1 part 1.1 fulfills the security objective. Lastly, SRP agrees the inclusion of “other methods” provides the necessary flexibility.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
a. Agree b. Agree c. Agree	

Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP recommends diagrams to be included in the technical rationale to more clearly illustrate how the concepts controlling essential logical connectivity within the LIZ would be applied to new and virtualization technology.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Security objectives add clarity, but I would add the language “R1 is intended to limit the ability of an attacker to move laterally throughout the secure environment” from the Technical Rationale in the requirement itself.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Security objectives add clarity, but I would add the language “R1 is intended to limit the ability of an attacker to move laterally throughout the secure environment” from the Technical Rationale in the requirement itself.	

Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Prater - Entergy - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer

Document Name

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

The SDT should provide more clarity around scripts and installed software. In CIP 007-7 Requirement R2.1, how is “essential” defined? Is the intent of this requirement to prohibit authorized users from writing and executing scripts in the course of their work? Is there a timeframe for alerting on newly-installed software or executable scripts? What does installed mean? If an executable or script is copied to the system, is it considered installed? Is a for loop typed in a shell considered a script? Would a shell alias be considered a script?

Likes 0

Dislikes 0

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer

Document Name

Comment

Seattle City Light contributed to and supports the comments provided by APPA.

Likes 0

Dislikes 0

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer

Document Name

Comment	
Button response should be "No". Button selection wasn't allowed. PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16. The SDT did a good job here. PAC believes it allows the flexibility to develop the program based on the infrastructure and how the communications are managed. {C}a) The security objective concept isn't new to cyber security controls. However, the subjectiveness will make it hard to audit as entities develop different implementations. It could open up an issue when the auditors develop an approach that identifies certain methods are more desirable than others and suggest entities adhere to their opinions rather than the language of the standard. {C}b) Excluding serial communications works, PAC understands the reasoning behind the change. Concern here is on Ethernet capable devices that aren't being used (RTAC, SEL-411, etc.) "Configure each system to provide only essential logical connectivity" Will we need to disable and document the port on the Cyber Assets in the Medium BCS? {C}c) Yes.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	
Document Name	
Comment	
Cowlitz agress with APPA comment.	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	
Document Name	
Comment	
APPA generally agrees that the proposed security objectives add clarity to the reason the requirement exists.	

Public power does have some general concerns with CIP-007. With the removal of the TFE language, is guidance anticipated on “per system capability?” The removal of the, “with External Routable Connectivity” makes this important for registered entities to understand. Also, there are concerns that the “Detect and alert on malicious communication within systems,” included within the Requirement Part on Connectivity.

A further public power concern is: will vendor supported applications be able to provide sufficient documentation related to the implementation of the multiple elements of the “Secure Configuration?” If this does not exist in an application, will companies have sufficient time to procure/develop such a system prior to compliance date?

Another potential issue for public power will be determining what is the intent of the note related to Secure Configuration for the CIP-007-7 R3 Part 3.2 “Mitigate the threat of detected malicious code.” We understand that we need to remove or isolate the detected malicious code, but how does the removal become part of the Secure Configuration of the BCS? The capability to detect the malicious code will exist in the antivirus solution. Where else is it likely to become part of the implemented configuration? How does it apply to virtual environments?

Proposed CIP-007 and CIP-010, have significant cross references and requirements related to the documentation of the Secure Configuration. APPA recognizes that this will require significant resource commitment to manage security controls in a traditional and virtual/cloud-based environment.

The new requirement introduced in part R2 should be limited in applicability to virtualized BCS and associated PCS. No technical basis is evident to justify the expansion of scope to include this new requirement for the existing approach to securing non-virtual BCS, etc. Although this practice might be a good security practice, CIP requirements are intended to provide a baseline of security practices not a collection of all good or best practices. Indeed, there exist many other good security practices that are not included in CIP requirements. It is not sufficient justification alone to add a new requirement just because it is a good practice; there should exist an overriding technical or security need. If this requirement is maintained, we recommend that it apply to virtualized BCS only.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

a. Yes

b. It appears that TFEs are being eliminated, is that true? Will guidance be provided to better clarify “per system capability” and the expected compliance documentation? How will this be audited if device capabilities within a system vary, or if a system is not capable? Specific guidance for Secure Configurations should be included. If entities are required to develop, this could be timely. “Detect and alert on malicious communication within a system” seems to be better suited for either R3 or R4.

c. Yes

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy believes that a response to question #8 (regarding IP/Serial Converter inclusion in BCS) to fully comment. Are Secure Configuration items required to be documented? We believe the fifth bullet in R2.1 is too vague (Other methods?) and will allow for interpretation differences between the auditor and the Registered Entity. Also, the new verbiage now says “per system capability” instead of “where technically feasible” in CIP-007…Does that mean that an entity can retire filed TFEs as long as they maintain evidence of system capability? i.e. the entity does not have to perform material change tasks with the regions anymore.	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO requests the SDT consider consolidating the requirements for Secure Configuration in a single Requirement or providing a Guidance Document.	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	No
Document Name	
Comment	
While we do not have specific comments on the questions proposed by the SDT, we do have concerns about certain updates within CIP-007. CIP-007 R1: For consistency, we suggest that the measure related to malicious commination under Part 1.1 be updated to include alerting or that alerting be removed from the requirement (“Detect and *alert* on malicious communication with systems”).	

CIP-007 R2: While we understand the reasoning behind the changes to R2, "controlling software that is allowed to execute on a BES Cyber Systems", there is some confusion on what the requirement means. For example, what does "essential software execution" mean? As tedious as it might sound, adding words such as "essential" into the requirements without explicitly expressing what the intent of the word is, causes issues with the entities and the regions. It would be prudent to get away from words that can be construed in different ways or that can change the execution of the requirement depending on how they are interpreted. Additionally, treating scripts the same as software, without further explaining what types of scripts, will cause undue burden on entities. For example, is it the SDT intent that read-only scripts be tracked? We believe that this could turn into a time-consuming task that will never be completed to an auditor or the requirements satisfaction.

Additionally, the Secure Configuration concept is found throughout CIP-007. Please see our comment relating to Secure Configuration under question 15.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy would like to comment the SDT for the work done in CIP-007-6, as we believe a movement to a risk-based approach for security will allow the flexibility to develop the program based on the infrastructure and how the communications are managed. In addition, with the removal of the strict timelines for R2, this would alleviate the multiple violations of this Requirement due to missing the 35 day windows, versus the intent of a program in preventing any incident due to the lack of patching Cyber Assets.

a) NV Energy does recognize that this more flexible approach to security does have its difficulties. The increase in subjectiveness will make it hard to audit as entities develop different implementations. It could open up an issue when the auditors develop an approach that identifies certain methods are more desirable than others and suggest entities adhere to their opinions rather than the language of the standard.

b) Excluding serial communications works, NV Energy understands the reasoning behind the change. Concern here is on Ethernet capable devices that aren't being used (RTAC, SEL-411, etc.) "Configure each system to provide only essential logical connectivity" Will we need to disable and document the port on the Cyber Assets in the Medium BCS?

c) Yes.

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	

Comment

CIP-007 R1 Part 1.1’s proposed wording appears ambiguous and confusing to us. The language of the requirement part does not contain the objective (where all of the other requirement parts in CIP-007 do contain the objective). Even though the security objective is present in the language of R1, it should be present in Part 1.1 as well, especially since R1.1 is after a page break.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 3	
Answer	No
Document Name	
Comment	
While the revised CIP-007 R2 is appropriate, it should be included in CIP-010 and it is a component of configuration management. Fullly support changes to requirement part 1.1, though additional guidance on how to demonstrate the requirement may be met is needed and agree that it will fill the objectives for virtualized systems.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
The structure of CIP-007 R1 requires mitigating risk of uncontrolled logical and phyicial connectivity which complicates the applicability table.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	

Comment

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 14.

Additionally, Westar | Kansas City Power & Light Company supplements the EEI response with the following observation:

The proposed revision raises questions as to whether moving patching to CIP-010 will mean patching is to be part of the CIP-010 "vulnerability management program" and no longer part of Security Configuration / Baselines.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

In general, comments made in response to Question 12 also apply to our concerns with CIP-007.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	No
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA).

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI

Answer	No
Document Name	
Comment	
Although adding security objectives does allow for flexibility in the technical approach taken to comply it also poses additional potential for disparate interpretations of the requirement between entities and auditors. An approach the entity feels addresses the objective adequately may be viewed by the auditor as unsatisfactory. A more prescriptive model lends to more concise interpretation of the requirements.	
Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
The structure of CIP-007 R1 requires mitigating risk of uncontrolled logical and phyicial connectivity which complicates the applicability table.	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF	
Answer	No
Document Name	
Comment	
ITC is in agreement with the comments submitted by EEI: "In general, comments made in response to Question 12 also apply to our concerns with CIP-007."	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	

Answer	No
Document Name	
Comment	
For Part 1.1, consider using “per system capability” instead of “excluding serial port connectivity such as RS-232 and RS-485.” Please clarify “Detect and alert on malicious communication within systems”. This basically calls for IDS at the hypervisor. Should this be in Requirement R3? Should this be something like limiting traffic? As written, Part 1.1 seems to imply that an entity would be required to implement all of the bulleted items if the system is capable. Please reconsider the wording of this. The note should not be used within requirement language in Part 1.1 and other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location. For Part 2.1, please provide clarification on executable scripts. This element continues to raise issues with disparate interpretations between entities and Regional Entities. A clear descriptor of this would aid in consistency of implementation across the industry. Consider using “available software” instead of “installed software”. There is software that can be usable without an actual installation process. Please clarify “essential”. Regarding Parts 3.1, 3.2, 4.1, 4.2, 5.1, 5.2, 5.5, 5.6, and 5.7, the note should not be used within requirement language in Part 1.1 and other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST supports the idea of adding security objectives to top-level (“R”) requirements, but believes, for R2, that the SDT needs to provide at least a working definition of “managed software” before establishing an objective of mitigation risks posed by “unmanaged” software. N&ST supports the goal of proposed R1 Part 1.1 modifications but believes that configuring applicable systems to permit only required logical/electronic communications should be mandatory, vs. only one of several acceptable options.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	

SMEC disagrees with the magnitude of changes to this standard. By removing “with ERC” from the applicable systems column of the requirement tables, multiple requirements will be added to the audit scope that were previously not applicable if there was no ERC. The LIZ should only apply to the virtual devices.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6

Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST and NPDD.

In addition, the following questions should be addressed or guidance provided to address some ambiguity:

- CIP-007 R1.1
    - “Excluding port connectivity such as RS-232 and RS-485.” Should other exemptions be provided, such as DNP3 using non-routable? Or instance when data is carried over a TCP/IP network that are serial at the end-point. Stated differently, remove the specific exemptions and state serial communications are exempted.
    - Explain why “ERC” was removed from the applicability.
- CIP-007 R2.1
    - Does “to allow only essential software execution” exclude firmware?
    - Are manual methods of alerting allowed? Can alerting be done on a periodic basis, or does this requirement require real-time alerting?
- CIP-007 R3.2
    - Are we required to identify and document the mitigation processes used on a BCS process, or is this requiring each mitigation activity be part of the Secure Configuration? Currently reads as the latter which is a CIP-008 issue. In addition, including response activities within the Secure Configuration does not provide any value to detecting cyber security incidents.
- CIP-007 R5.1
    - For Interactive User Access, it could be a process or technical control. How should a process be documented as part of the Secure Configuration, especially if the process allows for different approaches / solutions?
    - Adding administrative overhead to track this / could result in creation of numerous new CSI documents which poses a risk.
- CIP-007 R5.2
    - Adding administrative overhead to track this / could result in creation of numerous new CSI documents which poses a risk.

- CIP-007 R5.3-5.5
    - No comments
- CIP-007 R5.6
    - How should a process be documented as part of the Secure Configuration, especially if the process allows for different approaches / solutions?
    - Adding administrative overhead to track this / could result in creation of numerous new CSI documents which poses a risk

Likes 0

Dislikes 0

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO

Answer	No
Document Name	

Comment

Please see MRO NERC Standards Review Forum (NSRF) comments.

Likes 0

Dislikes 0

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5

Answer	No
Document Name	

Comment

PSE supports the comments developed by EEI.

Likes 0

Dislikes 0

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Support MRO NSRF comments

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

a. Agreed

b., c. Need further review.

Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer	No
Document Name	

Comment

NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations.

a) No.

b) No. We do not see a need to change R1. We also are concerned with adding the "detect and alert" language to Part 1.1. Adding the detecting and alerting seems to be duplicative with CIP-010 Part 2.1. Adding the "detect and alert" language increases compliance obligations for Medium Impact systems.

c) No. By adding this flexibility you also introduce auditor discretion into requirements that have very clear objectives. CIP-002-1 to CIP-002-3 required an entity to develop a Risk Based Assessment Methodology (RBAM) to determine Critical Assets. FERC did not agree with some entity assessments and requested the standard be changed to be more prescriptive. We now have the “Bright Line” criteria in CIP-002-5.1a. We think the risk assessment methodology provides the potential for relief of unnecessary burdensome work. The current requirements unintentionally require processes that do not make sense in certain circumstances but we think there is great risk of an auditor not completely understanding the entity’s risk and therefore issuing a PNC (Potential Non-Compliance).

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	AZPS Comments - Question 14.docx

Comment

Please see the attached document.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

Security objective-based requirements may be the right direction, but at the wrong time. Other non-NERC standards that are security objective-based are not subject to zero-defect compliance monitoring. In this case, security objective-based requirements may provide too much flexibility that could result in too much difference in interpretation between different Responsible Entities and auditors. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	

Dislikes 0	
Response	
Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	
Comment	
Adding the language to the Requirement does not make the Requirement objective based because the sub parts of the Requirement still need to be met.	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	No
Document Name	
Comment	
The proposed changes make progress toward accomplishing this goal, but they may also increase the compliance burden for existing BCS. Comments under question 9 apply here as well: The “ERC” qualifier has been removed from CIP-007 R1.1. This could dramatically increase burden on some entities, where the intended effect could be achieved instead with a virtualization-ready definition of “PCA” and “ERC.” CIP-007 R1.4 also seems to shift from requiring intrusion protection on an ESP level to requiring it on a BCS level. This will be onerous and may not be technically feasible in many cases, unless BCS are defined over-broadly (i.e., the entire LIZ is a single BCS). There is a meaningful distinction in keeping the BCS definition separate as a subcomponent of the LIZ. The appropriate shift would be from EAP to LIZ, not from EAP to BCS.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	

We disagree with these changes. We still support the current result-based requirements with appropriately prescriptive language. Even though the proposed objective-based non-prescriptive requirements provide some flexibility for the CIP compliance, they are too broad and subjective. By virtue of lack of detailed measures and guidance, how do the registered entities know their processes have been implemented effectively? How will Auditors/Teams be accredited to evaluate effectiveness? What will be the effectiveness metric? Given that currently the majority of CIP Cyber Assets are physical and the CIP compliance process today works fairly smoothly by implementing the existing requirements that are appropriately prescribed, it doesn't make sense to modify any existing requirements that are only for sufficing a small percentage of the virtual devices but a waste of the registered entities' time and resources for making these changes.

Resulting from our comments in the above question 1, as long as the virtual devices are identified correctly and the device-centric approach would still work well for the virtual devices, where the CIP-007 R1 Part 1.1 will apply to them smoothly.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to "what to do" not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

a. No.

b. No. The NSRF does not see a need to change R1. We also are concerned with adding the "detect and alert" language to Part 1.1. Adding the detecting and alerting seems to be duplicative with CIP-010 Part 2.1. Adding the "detect and alert" language increases compliance obligations for Medium Impact systems.

c. No. By adding this flexibility the SDT also introduces auditor discretion into requirements that have very clear objectives. CIP-002-1 to CIP-002-3 required an entity to develop a Risk Based Assessment Methodology (RBAM) to determine Critical Assets. FERC did not agree with some entity assessments and requested the standard be changed to be more prescriptive. We now have the "Bright Line" criteria in CIP-002-5.1a. We think the risk assessment methodology provides the potential for relief of unnecessary burdensome work. The current requirements unintentionally require processes that do not make sense in certain circumstances but we think there is great risk of an auditor not completely understanding the entity's risk and therefore issuing a PNC (Potential Non-Compliance).

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE does not agree CIP-007 needs to be changed with regards to virtual systems. Virtualized systems use ports and services just like physical systems and therefore they should all be evaluated and protected as they are currently. Texas RE has not seen issues specifically caused by virtualization using the current approach in CIP-007.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
We agree with some, but not all the modifications. We do agree that adding the security objectives in the requirements of CIP-007 is a step in the right direction. However, the requirements need to support defense in depth without penalty. For instance, in the modifications to CIP-007 R1.1, an entity can use a combination of four protections. If an entity employs two or more to an applicable system and one is found to have failed, then an Entity should not be found in violation if the other protection remained in place. The entity should only be found if violation if all protections for an applicable system related to R1.1 were not in place. Regarding modifications to CIP-007 R1.1, it is unclear if “Detect and alert on malicious communication within systems” actually meets the security objective of mitigating the risk posed by uncontrolled logical and physical connectivity. In addition, this is also a control for the security objective of mitigating the risk posed by malicious code in R3 and the security objective of monitoring security events to mitigate the risk posed by detectable security incidents in R4. So, if an entity chooses only this control for a system then they are potentially also in violation of R3.1 and R4.2.1. Either the mitigation measure needs to belong only to one security objective to avoid multiple violations if one fails, or the entire CIP-007 needs to be reworked to a program that addresses each risk and the entity has identified controls for each risk. Again, with the idea that an entity with multiple controls in place for a particular risk is not penalized when one control fails, but other controls remain in place. The proposed changes might provide a degree of future proofing, but per Master Yoda, “Difficult to see. Always in motion is the future.”	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	

Answer	No
Document Name	

Comment

No, NRG does not agree that adding the security objectives throughout the Requirements in CIP-007 adds clarity to the reason the requirement exists, because the new secure configuration definition mandates malware monitoring within BES Cyber Systems which implies AV on the BCS and not at the system level (which is the only requirement of the current standard). This proposed change could also imply needing network access control, whitelisting, and/or needing host based intrusion detection.

No, NRG does not agree that the proposed security objective in CIP-007 R1, "to mitigate the risk posed by uncontrolled logical and physical connectivity" because it expands the port control requirements. Registered entities that have used no ERC as a security measure,will now have additional compliance requirements. The security gained from these activities may not outweigh the additional compliance burden to the industry. NRG does not agree that the modifications to CIP-007 R1 Part 1.1 fulfill this security objective for systems where connectivity is not limited to TCP/IP port service combinations, as in virtualized systems and SAN based storage because The new secure configuration definition mandates malware monitoring within BES Cyber Systems which implies AV on the BCS and not at the system level (which is the only requirement of the current standard). This proposed change could also imply needing network access control, whitelisting, and/or needing host based intrusion detection.

No, NRG does not agree that the modifications to CIP-007 R1 Part 1.1 add necessary flexibility to fulfill the security objective of CIP-007 R1 for virtualized systems and provides a degree of future proofing because while the direction of the other version 7 standard revisions have shifted focus to a system, this requirement provides a vague approach with underlying expectation on cyber asset level protections. Many control system vendors do not currently support host-based firewalls and/or intrusion detection systems. The same protection could be realized at the system level through a combination of firewalls, intrusion detection, configurations monitoring, network access control, malware scanning, and TCA/RM controls.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

For Part 1.1, consider using "per system capability" instead of "excluding serial port connectivity such as RS-232 and RS-485." Please clarify "Detect and alert on malicious communication within systems." This basically calls for IDS at the hypervisor. Should this be in Requirement R3? Should this be something like limiting traffic? As written, Part 1.1 seems to imply that an entity would be required to implement all of the bulleted items if the system is capable. Please reconsider the wording of this. The note should not be used within requirement language in Part 1.1, or in other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location.

For Part 2.1, please provide clarification on executable scripts. This element continues to raise issues with disparate interpretations between entities and Regional Entities. A clear descriptor of this would aid in consistency of implementation across the industry. Consider using "available software" instead of "installed software." There is software that can be usable without an actual installation process. Please clarify "essential."

Regarding Parts 3.1, 3.2, 4.1, 4.2, 5.1, 5.2, 5.5, 5.6, and 5.7, the note should not be used within requirement language in Part 1.1, or other requirements. As written, this is not an actual requirement. It is simply guidance in this format. The content should be moved to a more appropriate location.

Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
In general, comments made in response to Question 12 also apply to our concerns with CIP-007.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Hydro One supports the comments submitted by NPCC TFIST.	
Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	

Comment

In order to provide the necessary flexibility to fulfill the security objectives and to clarify ability to choose, please consider adding "or" at the end of each line of all bullet point lists providing options.

R1.1 recommended updated language reads:

• Configure each system to provide only essential logical connectivity; or

• Detect and alert on malicious communication within systems; or

• Baseline system logical connectivity, and alert on deviation from baseline; or

• Other method(s) to mitigate the risk posed by uncontrolled logical connectivity.

R2.1 recommended updated language reads:

• Configure each system with intentionally installed essential software and executable scripts; or

• Baseline currently installed software and executable scripts and alert on any newly installed software or executable scripts; or

• Implement application whitelisting; or

• Use read-only bootable media; or

• Other methods to mitigate the risk posed by unmanaged software.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	No
Document Name	

Comment

We disagree with the removal of “with External Routable Connectivity” as an applicable system in CIP-007.

Is CIP-007 R1 1.1 only applicable to systems where there is virtual technology? If so shouldn't that be listed as the applicable system? R1 is to mitigate the risk posed by uncontrolled logical and physical connectivity; Part 1.1 doesn't address physical and logical connectivity.

In CIP-007 2.1 – How would this apply to a BES Cyber System that is a System Protection Relay?

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA

Answer No

Document Name

Comment

Adding the language to the Requirement does not make the Requirement objective based because the sub parts of the Requirement still need to be met.

Likes 0

Dislikes 0

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group

Answer No

Document Name

Comment

a. The SSRG requests the Standard Drafting Team ensure the language is clear enough to allow the Reponsible Entity to have clear direction what consistutes the type of port that is included in the Secure Configuration. For example, unlike CIP-007-6 which utilizes more concise language such as "logical network accessible ports that have been determined to be needed by the Responsible Entity…", version 7 utilizes terminology such as "only essential logical connecticity" and "uncontrolled logical connectivity," and states the standard excludes serial port connectivity "such as RS-232 and RS-485." This language appears very broad and subjective to what is included.

b. The SSRG does not see a need to change R1. Adding the "detect and alert" language to Part 1.1 seems duplicative of CIP-010 Part 2.1 and increases compliance obligations for Medium Impact systems.

c. The SSRG is concerned that by adding the referenced flexibility, auditor discretion is introducted into requirements that have very clear objectives. CIP-002-1 to CIP-002-3 required an entity to develop a Risk Based Assessment Methodology ("RBAM") to determine Critical Assets, which includes the "Bright Line" criteria in CIP-002-5.1a. The SSRG believes the RBAM approach provides for relief from unnecessarily burdensome work and mitigates auditor discretion.

Likes 0

Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

MRO does not agree with these changes because it is not clear how “Mitigate the Risk” language supports enforceable requirements for the system security management of BES Cyber Systems. “Mitigate the risk” could be interpreted as anything between “Eliminate the Risk” and “Detect the Risk”. This could lead to challenges in consistent CMEP implementation by the ERO.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company requests clarification on the interplay between the objective in the overall requirement and the scoping of applicability in the table. As an example, CIP-007 R1 addresses mitigating the risk posed by uncontrolled logical and physical connectivity, yet the physical connectivity mitigation in the table is scoped to high impact control centers only. If an entity has only medium impact systems, what is the obligation of this requirement? The main requirement states they must implement a process that mitigates the risk posed by uncontrolled logical and physical security - and that plan(s) "collectively include" the requirement parts, but it does not state or clarify that it is *scoped* by those parts. This was not an issue previously as all the objectives and requirements were in the tables. It has changed now that the objective is in the overall requirement. Southern suggests the SDT consider this issue across all the standards and clarify how the high-level objectives work with the applicability column in the tables.

Logical connectivity in CIP-007 R1.1 – does this unintentionally alter the scope for ports and services? This is a backwards compatibility question. Southern would like to see additional clarity in the definition for logical connectivity. This terminology is used throughout these proposed changes and clarity in the application of this term can provide clarity in scoping.

Can this unintentionally scope in “anything connected to the system”? Will mounting a drive unintentionally scope in that logical connectivity? Do we have to start tracking (i.e. making lists) of everything that a system connects to? How might this extend into shared memory? Do we need to enumerate USB mice and keyboards?

Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	

15. The SDT is proposing modifications to CIP-010 (see the CIP-010 Technical Rationale document for detailed information.). Do you agree with these changes? Please provide comments to support your response. In particular, the SDT seeks stakeholder feedback on:

a. The SDT is proposing adding the security objectives throughout the Requirements in CIP-010. Do you agree that the proposed security objectives add clarity to the reason the requirement exists?

b. The SDT is proposing to modify the referenced baseline configuration from CIP-010-3 R1 Part 1.1 to a 'Secure Configuration' which is made up of the implemented controls that fulfill requirements within CIP-005 and CIP-007. Do you agree that this set of controls supports managing change under CIP-010 R1 Part 1.1?

c. The SDT is proposing to modify the current CIP-007 R2 requirements and move them to CIP-010 R3. The SDT believes that the software vulnerability management found within this set of requirements fits logically within the security objective of CIP-010 R3 "to mitigate the risk posed by system vulnerabilities" and has moved it there. Do you agree?

d. The SDT is proposing CIP-010 R3 Parts 3.5 and 3.6 to replace the current CIP-007 R2 Parts 2.1 – 2.4. Do you agree that the proposed CIP-010 R3 Parts 3.5 and 3.6 offer the additional flexibility needed when implementing virtualized systems that can be dormant for a period, and for which security patches have become available?

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

We still recommend to provide a minimum required 12 month vulnerability assessment and not solely base it on risk for R3 Part 3.6

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	Yes
Document Name	

Comment

MISO supports the shift to risk-based implementation time frames.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

a) Yes, the additions help clarify intent. As with any compliance standard, it is important to integrate the intent with the method of auditing to allow the intent to be the focus and not prescriptive details. This also needs to be clearly and consistently communicated throughout the regions.

b) Yes.

c) Yes.

d) Yes.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

Regarding b: Entities will need to track the Secure Configurations in a similar way to current baselines (with OS, software, etc) to monitor for and react to potential incidents and vulnerabilities. Additionally, tracking this way will assist entities in identifying, isolating and/or patching potentially vulnerable physical or virtual BCS.

Regarding d: This will require an entity to provide a thorough explanation of their rationale behind the periodicity for identifying software vulnerabilities.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance

Answer	Yes
Document Name	

Comment

No comment.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

See previous comments regarding BCS and LIZ definitions

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3

Answer	Yes
Document Name	

Comment

In response to part C, Hydro One supports moving Patch Management program from CIP-007 to Vulnerability Management in CIP-010. Patches remediate vulnerabilities, but vulnerabilities can exist without a patch to remediate, so other mitigation maybe necessary.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	Yes
Document Name	

Comment

Security Objectives do add clarity. Moving security patching to the Secure Configuration makes sense.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Security Objectives do add clarity. Moving security patching to the Secure Configuration makes sense.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Junji Yamaguchi - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nathaniel Clague - Portland General Electric Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0

Dislikes 0

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer

Document Name

Comment

Seattle City Light contributed to and supports the comments provided by APPA.

Likes 0

Dislikes 0

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer

Document Name

Comment

Button response should be "No". Button selection wasn't allowed.

PacifiCorp’s approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be covered in question #16.

The SDT did a good job here. PAC believes it allows the flexibility to develop the program based on the infrastructure and how the communications are managed.

{C}a) The security objective concept isn’t new to cyber security controls. However, the subjectiveness will make it hard to audit as entities develop different implementations. It could open up an issue when the auditors develop an approach that identifies certain methods are more desirable than others and suggest entities adhere to their opinions rather than the language of the standard.

Secure Configuration (proposed) The implemented set of controls supporting the security objectives found within the CIP Reliability Standards where the following text exists within the requirement language: “NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system.” New “Baseline” = CIP-005 R1.1, CIP-007

{C}a) R1.1, R2.1, R3.1, R3.2, R4.1, R4.2, R5.1, R5.2, R5.5, R5.6, R5.7, CIP-010 R3.6. This concept makes sense, but would need further review as compared to the original CIP-010 Bassline and CIP-007 controls documentation to fully understand the impacts of the changes proposed.

{C}b) From the beginning of CIPv5 that Patch Management should be CIP-010, PAC agrees with this change. Not understanding the new phrase “The process requirements of Part X.X and timeline are based on the analysis of the risks to BES reliability and the risks posed by the …”. Is the SDT expecting a risk register and program with thresholds of when things need to be done? Seems like this could be a good thing if we embrace this idea, but it leaves the auditors to determine what they feel is reasonable too when checking whether the timelines indicated line up with the risk level identified. Are there plans for future development during the drafting that the SDT plans to add some timeframes into the standards like before (i.e. every 35 days, etc.)

{C}c) Yes, PAC believes the SDT did a good job moving this to CIP-010 and allowing for flexible schedules based on system activity. However, our concern with timelines and risk are the same as explained in item "C" above.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

Public power agrees with transferring the requirements from CIP-007 to CIP-010 as mitigating software vulnerabilities more closely relates to vulnerability management rather than system management. However, as the 4 parts of this question suggest, these modifications add complexity to the standard. For example, the definition of the new term Secure Configuration and its role is unclear, and stakeholders can envision the term taking on more significance in the future. While it seems appropriate to identify the security controls as part of the Secure Configuration, some Entities had implemented the requirements for the current CIP-010 security controls by evaluating changes against all CIP-005 and CIP-007 security controls. Consequently, it would be best for the SDT to list out what the Secure Configuration is composed of.

APPA does consider that the move of the CIP-007 R2 requirements to CIP-010 is an improvement by locating them in a single standard. They are logically part of the methods that industry uses to mitigate the risk of system vulnerabilities. Further, we agree that the proposed changes will provide flexibility for virtual systems.

Although the Secure Configuration concept is not fully understood, either in application or audit approach, there is reasonable concern that it expands the scope of requirements for non-virtualized BCS. See further discussion above in responses to Question 14. Under the principle that CIP scope generally should not be expanded in these revisions for non-virtualized systems, the dual-definition/dual-requirement "overlay" approach discussed in Question 3, above, may be warranted as a means for entities to remove the scope expansion for existing BCS, for which the existing baseline approach may be sufficient.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10

Answer	
Document Name	

Comment

abstain

Likes 0	
Dislikes 0	

Response

Russell Noble - Cowlitz County PUD - 3,5

Answer	
Document Name	

Comment

Cowlitz agrees with APPA comment.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6

Answer	No
Document Name	

Comment

NYPA supports comments submitted by NPCC / TFIST.

In addition, the following questions should be addressed or guidance provided to address some ambiguity:

- CIP-010 R1.1
    - Need to provide guidance on how timelines should be developed and what the risk analysis needs to consider. Is the entity required to develop their own risk analysis or will guidance be released making this more prescriptive? Will the resulting entity risk assessment process / criteria be subject to auditors?
    - Why does the requirement exclude EAMS and PAMS? Security controls should be applied to these systems that log and monitor. Not doing so will reduce security posture and make it difficult to meet requirements under CIP-006, 7 and 8.
- CIP-010 R1.2
    - Why is R1.2 written to CIP-005 and CIP-007 controls, whereas R1.1 is written to the Secure Configuration? This seems to be an inconsistency that should be addressed, or at a minimum explained.
- CIP-010 R1.3

  - Is firmware and operating system exempted since it is not included within R1.3.1 and R1.3.2 requirement text?

- CIP-010 R2
  - Similar question on timelines. Also, why is impact rating called out in the bottom note when the only applicable impact rating is High Impact? How many different types of risk assessments need to be conducted across CIP-010?

- CIP-010 R3.5
  - Is software intended to include firmware and operating systems? Firmware and operating system is called-out in CIP-010 R1.3 but not here. Why the inconsistency?
  - Similar comment on conducting risk assessments. If 35-days was sufficient under CIPv5, is it also sufficient under this proposed revision, thereby not requiring a risk assessment?

- CIP-010 R3.6
  - Is software intended to include firmware and operating systems? Firmware and operating system is called-out in CIP-010 R1.3 but not here. Why the inconsistency?
  - Similar comment on conducting risk assessments. If 35-days was sufficient under CIPv5, is it also sufficient under this proposed revision, thereby not requiring a risk assessment?

Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	No
Document Name	
Comment	
SMEC disagrees with these changes. SMEC believes the change from Configuration Baseline to Secure Configuration and additional requirement for risk assessment exceed the mandate from the SAR and will be an unnecessary burden to industry. More detail on measures and guidance would be needed for such substantial changes.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	

Comment

N&ST supports the addition of various types of applicable system configuration data to what is presently referred to as a “baseline configuration.” However, N&ST opposes changing the name to “Secure Configuration,” as it would not, by itself, contribute to the goal of making BES Cyber Systems as resistant to attack as possible. What it would do, instead, would be to compel all Responsible Entities to overhaul their existing CIP-010 documentation.

>> N&ST supports moving the existing CIP-007 R2 (patch management) requirements to CIP-010. N&ST also supports the goal of moving away from a calendar-driven, “apply all security patches” approach to vulnerability management. However, N&ST is concerned that some entities may lack the expertise necessary to perform comprehensive vulnerability management on an ongoing basis, and that among those that lack such skills, they could face tough questioning from audit teams. N&ST recommends adding some “… using one or more of the following approaches” language to the requirement language. An example might be, “By assigning security patching or mitigation action schedule priorities based on vulnerability severity ratings assigned by agencies such as the U.S. CERT.” N&ST is also concerned that while attempting to make CIP requirements generally less prescriptive, the SDT may have moved the pendulum too far: N&ST believes that allowing entities to to establish their own timetables for performing vulnerability identification and mitigation tasks incurs the risk of wide variations across the industry. N&ST has similar concerns about proposed changes to configuration monitoring requirements.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES

Answer	No
Document Name	

Comment

The use of software throughout the Standard, like in 1.3, 3.5, and 3.6 is inconsistent with the requirements of R1.3 “operating system, firmware, and software”. Are we to assume that the term software actually means “operating system, firmware, and software”? Maybe a defined term is needed?

The Secure Configuration definition is challenging us. Our preference woudl be that the definition did not referencing a set of standards, rather it were just fully defined. Also, we find this “NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system” text in CIP-010 R3.6 and I can’t trace back from that what the definition is.

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

The parts of Requirement R1 could be improved by putting the parts in sequence with actual change control (eg, implement in test, security controls testing, approve for production, etc.). As written the requirement is difficult to follow. The last statement in Part 1.1 should be guidance. It is not written as an objective requirement.

The last statement in Parts 2.1 and 2.2 should be guidance. They are not written as an objective requirement.

Requirement R3 is a good change over the current approach to patching. However, these changes may require significant significant capital investment and process changes. Requirement Part 3.6 should include provisions for changing a mitigation plan, similar to the current requirement in CIP-007 R2. This would allow entities to address changes in their timeline without the risk of a violation.

Likes 0

Dislikes 0

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer	No
Document Name	

Comment

ITC is in agreement with the comments submitted by EEI:

"EEI’s concerns over the proposed changes to CIP-010 align with our comments and concerns as described for Questions 12."

Likes 0

Dislikes 0

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

The approach is good, but the scope and impact to existing operations is profound.

Likes 0

Dislikes 0

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	No
Document Name	
Comment	
Although adding security objectives does allow for flexibility in the technical approach taken to comply it also poses additional potential for disparate interpretations of the requirement between entities and auditors. An approach the entity feels addresses the objective adequately may be viewed by the auditor as unsatisfactory. A more prescriptive model lends to more concise interpretation of the requirements.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP	
Answer	No
Document Name	
Comment	
Lakeland Electric supports the comments provided by the American Public Power Association (APPA).	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
Exelon’s concerns over the proposed changes to CIP-010 align with our comments and concerns as described for Questions 12.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	

Answer	No
Document Name	
Comment	

Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute's response to Question 15.

Additionally, Westar | Kansas City Power & Light Company share the following concerns.

Proposed Glossary Term, Secure Configuration, is ripe with compliance ambiguity and confusion. The Glossary Term can be interpreted as without boundaries. Recognizing flexibility in Standards and definitions is desirable, there is a need to provide a parameter, a fence, in which to operate.

Also, propagating into each CIP Standard is not required. Secure Configuration is restating a basic precept of compliance--establish and implement controls. Reiterating a fundamental principle of compliance does not promote compliant behavior nor improve reliability of the BES.

Finally, compliance ambiguity creates inconsistency in the CMEP.

Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	No
Document Name	
Comment	

The approach is good, but the scope and impact to existing operations is profound.

Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 3

Answer	No
Document Name	
Comment	

Agree with additions to adding security objectives to CIP-010.

The definition of secure configuration is not adequately stated. This will either need to be fully prescriptive or fully non-prescriptive to be successful. While the fully non-prescriptive route would be preferred, this may result in an unenforceable standard.

Agree with moving CIP-007 R2 to CIP-010.

While conceptually supporting the changes, the details of how to comply with CIP-010 R3.5-3.6 are not adequately defined. Please provide clear guidance how to meet the standard and consider language changes to support the intent.

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	

Comment

In general, as proposed, the Secure Configuration concept seems problematic   The Secure Configuration now contains many new elements not previously tracked through the baseline configuration. Many of these additions are potentially difficult to inventory (for example, logging and alerting configuration may be distributed throughout multiple systems, such as local application configuration, AD Group Policy and SEIM configuration, which is spread across multiple asset classifications).   Particularly with CIP-007 R4 and the changes to EACMS, some of these Secure Configuration items may be changes to non-applicable Systems (as SEIMs will in general be out of scope for CIP-010 R1, but the BES Cyber System’s configuration for logging and alerting, which is required to be part of the Secure Configuration, will reside on this out of scope device).

Several of the requirements (CIP-007 R3.2 and the procedural aspects CIP-007 R5.5 and R5.6) are procedural in nature. It does not make sense to include these in a Secure Configuration, as the actual configuration of the associated system is not changing when a change to these procedures is made.

Additionally, some of the requirements (CIP-007 R5.1 and CIP-007 R5.2 marked to be part of the secure configuration seem at best redundant. These items rarely change, and usually not at the behest of the Responsible Entity, RE, (the methods of authentication rarely change from deployment; changes to the default account inventory are usually due to a vendor disclosure of an undocumented account). As such, it does not really make sense to include these in the Secure Configuration, requiring regular monitoring and inventory.

In CIP-010 R3.6, the requirement allows for other means to mitigate a vulnerability besides the installation of security patches. This would now require CIP-010 change control for changes that might be covered by other CIP requirements (requirement not already part of the secure configuration), or even outside the standards. This greatly increases the burden of CIP-010 R1 on REs.

Another problem with the current proposal is that the way the “Secure Configuration” tag is applied to the requirements can be ambiguous. For example CIP-010 R3.6, which requires the RE to “Create or update a plan to mitigate the identified software vulnerabilities…” includes the Secure Configuration tag. The question becomes is the plan part of the Secure Configuration, or the security patches/mitigations implemented? Once again, procedural methods may fall into the scope of the Secure Configuration.

Finally, the SDT suggests in the Rationale that the expansion the of Secure Configuration beyond the currently implemented items in CIP-010-2 R1 Part 1.1 is needed due to the greater risks posed by virtualization. Yet there is no accounting for risk for purely physical systems, and potentially the compliance burden might even be higher given the lack of a centralized management platform on physical systems. This would place an undue burden upon entities who choose to remain physical rather than adopt the complexities of virtualization

CHPD would like to see the removal of the Secure Configuration tag from CIP-007 Requirement Parts R3.2, R4.1, R4.2, R5.1, R5.2, R5.5, and R5.6. Additionally, CHPD would like the Secure Configuration to be made more granular to only apply to actual configuration on applicable systems for all requirements (such as installed patches for CIP-010 R3.6 or local configuration changes).

CHPD support the changes moving CIP-007 R2 to CIP-010 R3.5 and R3.6 as well as the changes made (with the exception of the Secure Configuration tag).

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy does not support a major overhaul of the standards at this time. However, if the SDT continues to make revisions, CenterPoint Energy recommends the following:

CenterPoint Energy supports the flexibility of the timeframes being determined by Entity. However, below are questions that need clarification:

- Where is the line between changes required for incident response and the change control process required in CIP 010-4 Requirement R1?
- Is authorization required prior to the remediation step in an incident response plan?
- The CIP 010-4 Requirement R1.1 requirements may have the inadvertent impact of slowing down incident response. Can IR policies be customized to pre-authorize remediation changes?

The removal of Requirement R1.2 requiring authorization without reference to timeframe may hinder timely incident response. With this new change, entities are tied to pre-authorization of any change and potentially penalized for acting in response to operational or security circumstances.

Changes to CIP-010 Requirement R1.3 do not exclude installation of signatures addressed in CIP-007 Requirement R3. While it is important to validate software, this requirement may impede timely implementation of signature based security controls even more than the current CIP-007 Requirement R3 requirements do. This entity recommends excluding signatures in this requirement to allow entities the flexibility to automate signature updates without retaining records of hash verifications for each transaction.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

NV Energy does recognize that this more flexible approach to security does have its difficulties. The increase in subjectiveness will make it hard to audit as entities develop different implementations. It could open up an issue when the auditors develop an approach that identifies certain methods are more desirable than others and suggest entities adhere to their opinions rather than the language of the standard.

NV Energy is unable to provide a effective evaluation for this question at this time, due to the extent of the “Secure Configuration” spanning multiple Requirements in CIP-005 and CIP-007. Further review will be needed to determine the impact of this new model.

NV Energy would like to comment the SDT for the work done in CIP-010, as we believe a movement to a risk-based approach for security will allow the flexibility to develop the program based on the infrastructure and how the communications are managed. In addition, with the removal of the strict timelines from CIP-007-6 R2, and moving to a risk based approach for review in CIP-010, this would alleviate the multiple violations of this Requirement due to missing the 35 day windows, versus the intent of a program in preventing any incident due to the lack of patching Cyber Assets.

NV Energy does agree with this approach for addressing virtualized systems in CIP-010 R3, P3.5 and P3.6

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	No
Document Name	

Comment

a. We agree that the proposed security objectives add clarity to the reason the requirement exists.

b. While we agree with the SDTs approach to not include the long list of requirements associated with Secure Configuration in the definition or in CIP-010, we do not agree with the concept of Secure Configuration. The move from Version 3 to CIP Version 5 saw the elimination of almost all of the “spaghetti requirements” with the expectation of CIP-010 R1, which, in essence, was just a documentation exercise. This was a welcome change and eliminated a lot of confusion. The addition of the Secure Configuration concept, and the combined 13+ parts, feels like the industry is going backwards and not forwards. In short, this is a documentation nightmare that has no benefit for the entities or the BPS. Furthermore, tracking and monitoring several of the items within the Secure Configuration seems time intensive or not feasible. We propose that the SDT continue to consider how CIP-010 could become a more objective-based reqruiement, instead of the currently proposed prescriptive-based requirement, and also focus on eliminatating the risk associated with creating “spaghetti requirements” and the administrative burden that comes with an inordinate amount of compliance documentation without a security benefit.

c. While we agree that focusing on software vulnerabilities is an improved approach, we believe that the requirement as written can cause additional confusion. For example, if an entity’s program is based on security patches and there is a software vulnerability that has been publicized and yet has no associated security patch, is the entity required or expected to implement a “plan to mitigate the identified software vulnerability”? We believe as written, the entity could say no to the question above (there is no patch therefore they have not identified a vulnerability) but an auditor could argue that they are out of compliance. Additionally, focusing on just software vulnerabilities could lead some entities to feel pressure to apply “hot fixes” to their environment which could cause severe reliability issues for the BPS.

Likes 0	

Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
It doesn’t appear there is a requirement to document the Secure Configuration. Is this the case? Is R1.1.1 requiring Authorization prior to the change being implemented? Should R1.3 be implemented Secure Configuration instead of existing? R2.1 – What is the difference between Configuration monitoring and Configuration auditing? R3.3 – R3.2 allows for “per Cyber Asset capability” but R3.3 does not. Without timeframe expectations in R3, the opportunity for interpretation differences between the auditor and RE may exist.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
It makes sense to move CIP-007 R2 to CIP-010. The elimination of the 35-day timeframe requirement for patching and moving toward a risk-based assessment methodology, while makes sense, poses concerns about how this will be audited. The risk in allowing entities to manage vulnerabilities based solely on risk may alter accountability in assessing and applying patches in a timeframe viewed acceptable by auditors.	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP is in agreement with the concept of raising the Requirements to an objective level. However, we have concern for the proposed movement of the vulnerability management requirements from CIP-007 to CIP-010. Our belief is that CIP-010, as it is today, is essentially a quality assurance standard	

established as a means for confirming all the vulnerabilities “have been managed” not for requirements “to manage” vulnerabilities. AEP requests that the SDT consider retaining CIP-010 in this role by returning proposed CIP-010-4 Requirement Parts 3.5 and 3.6 to their former place in CIP-007. And, AEP requests specific examples of the intended implementation of ‘Secure Configuration’ be included in the technical rationale to provide more clarity of how this concept will reduce administrative burden in complying with the CIP standards.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry’s programs. Originally, there was the Version 5 Transition Advisory Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change.   The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to “what to do” not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

a. No.

b. Yes. However, this change will increase the number of Cyber Asset attributes that need to be tracked for what was previously baseline attributes and will increase the compliance risk for change control. For instance, if a new generic account is added to a Cyber Asset (common operator account), current requirements are to identify and inventory the account. The proposed requirement makes this part of the Secure Configuration which will require the addition of the account to follow CIP-010-4 Part 1.1 change control processes. Currently, following your CIP-010-2 change control process is a best practice; it is not a violation if you do not follow it when adding a new generic account. This is just one example. Creating the new Secure Configuration definition and tying the definition to CIP-010-4 will significantly increase compliance work and introduces concern with auditor discretion.

c. No. We don’t think it matters which standard, CIP-007 or CIP-010, the requirements reside. Moving the requirements will cause unnecessary documentation changes.

d. No. We think the new requirements add the ability for auditor discretion to requirements that were previously very clear. For instance, if an entity chooses to only monitor patch sources (Part 3.5), it would reason that if no security patches are released there would be no requirement to have a mitigation plan. However, if an entity chooses to monitor patch sources as well as monitor a vulnerability database (Part 3.5), a mitigation plan would be required if a vulnerability is discovered in the database even though there is no patch released for the vulnerability. An auditor may view this as a weak program and issue a PNC.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	
We disagree with these changes. We still support the current result-based requirements with appropriately prescriptive language. Even though the proposed objective-based non-prescriptive requirements provide some flexibility for the CIP compliance, they are too broad and subjective. By virtue of lack of detailed measures and guidance, how do the registered entities know their processes have been implemented effectively? How will Auditors/Teams be accredited to evaluate effectiveness? What will be the effectiveness metric? Given that currently the majority of CIP Cyber Assets are physical and the CIP compliance process today works fairly smoothly by implementing the existing requirements that are appropriately prescribed, it doesn't make sense to modify any existing requirements that are only for sufficing a small percentage of the virtual devices but a waste of the registered entities' time and resources for making these changes. Resulting from our comments in the above question 1, as long as the virtual devices are identified correctly and the device-centric approach would work well for the virtual devices, where all existing requirements of CIP-007 and CIP-010 will apply to them smoothly.	
Likes 0	
Dislikes 0	
Response	
Joseph Pride - Trans Bay Cable LLC - 1 - WECC	
Answer	No
Document Name	
Comment	
The new CIP-010 provides a logical configuration control framework that can be extended to cover future Requirements without requiring a revision of CIP-010. The proposed changes do significantly increase the scope of configuration change control. However, this increase in scope may not be entirely onerous; management controls corresponding to the Secure Configuration already need to be implemented in some form to ensure compliance with the corresponding Requirements. While the new language does provide flexibility, some of that flexibility comes with compliance uncertainty. Where process requirements and timeline are based on risk analysis, significant additional definition is needed around what is acceptable for a risk analysis and how it shall be determined; this language leaves the door wide open for entities to give themselves the broadest interpretation of the gray area internally, resulting in unresolvable disagreements upon audit. To provide reasonable assurance, a separate Requirement or even a separate Standard may be required for defining risk analysis, similar to how CIP-002 defines Impact Rating. A clear distinction may need to be drawn between Impact Rating and risk analysis. As an alternative, a collaborative process may need to be formally defined and required outside of the audit process, in which the risk analysis methodology is reviewed and approved by the RRO, and the analysis itself may require a form of interaction with the RRO.	
Likes 0	
Dislikes 0	

Response	
Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	No
Document Name	
Comment	
Moving to a security objective approach implies for a need for a cyber-security plan which considers the risk and appropriate mitigation and controls to meet the objective.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	
Comment	
Security objective-based requirements may be the right direction, but at the wrong time. Other non-NERC standards that are security objective-based are not subject to zero-defect compliance monitoring. In this case, security objective-based requirements may provide too much flexibility that could result in too much difference in interpretation between different Responsible Entities and auditors. The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues. It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment	
a. Agree b. Agree c. Agree d. Disagree. The question d) seems to indicate that the intention of the SDT is that patches must be applied to dormant systems. This might not be desired if dormant instances are serving as backups to a production instance (for CIP-009 purposes). Flexibility is needed to allow for dormant intances/ systems to remain as is and only apply patches if the dormant instance is reused as a production instance (CIP-010 R1.2).	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	AZPS Comments - Question 15.docx
Comment	
Please see the attached document.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
NPPD does not support the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. The changes being proposed present a risk of unintended consequences for what is the vast majority of systems that are not in virtualized environments. NPPD provides our comments in the spirit of identifying some of the risks and unintended consequences for moving forward in this direction; and in the final comment on this form our recommendations. a)No.	

b) Yes. However, this change will increase the number of Cyber Asset attributes that need to be tracked for what was previously baseline attributes and will increase the compliance risk for change control. For instance, if a new generic account is added to a Cyber Asset (common operator account), current requirements are to identify and inventory the account. The proposed requirement makes this part of the Secure Configuration which will require the addition of the account to follow CIP-010-4 Part 1.1 change control processes. Currently, following your CIP-010-2 change control process is a best practice; it is not a violation if you do not follow it when adding a new generic account. This is just one example. Creating the new Secure Configuration definition and tying the definition to CIP-010-4 will significantly increase compliance work and introduces concern with auditor discretion.

c)No. We don't think it matters which standard, CIP-007 or CIP-010, the requirements reside. Moving the requirements will cause unnecessary documentation changes.

d)No. We think the new requirements add the ability for auditor discretion to requirements that were previously very clear. For instance, if an entity chooses to only monitor patch sources (Part 3.5), it would reason that if no security patches are released there would be no requirement to have a mitigation plan. However, if an entity chooses to monitor patch sources as well as monitor a vulnerability database (Part 3.5), a mitigation plan would be required if a vulnerability is discovered in the database even though there is no patch released for the vulnerability. An auditor may view this as a weak program and issue a PNC.

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

: a. Agreed

b., c., d. Need further review.

Likes 1	PSEG, 1,3,5,6, Cavote Sean
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP does not agree or disagree that the proposed security objectives add clarity to the reason the requirement exists. SRP agrees with transferring the requirements from CIP-007 to CIP-010 as mitigating software vulnerabilities more closely relates to vulnerability management rather than system management.

However, SRP asserts the Secure Configuration definition needs more clarification. To understand the components of Secure Configuration, Responsible Entities would need to sift through the requirements. It should be clearly stated in the definition what the Secure Configuration is composed of.

Likes 0	
Dislikes 0	

Response

Jamie Prater - Entergy - 5,6

Answer	No
Document Name	

Comment

Entergy feels that the proposed changes to CIP-010 increase the scope of CIP-010 to an extent where those changes may be redundant with other requirements such as CIP-005-7 R1.1, CIP-007-7 R1.1, R2.1, R3.1, R3.2, R4.1, R4.2, R5.1, R5.2, R5.5, R5.6 AND R5.7. These redundancies would need to be resolved by modifications to or eliminations of those other requirements.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Support MRO NSRF Comments

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
PSE supports the comments developed by EEI.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	
Answer	No
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports the comments made by EEI and the Long Island Power Authority.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No

Document Name

Comment

Southern Company generally agrees with the direction, but has several concerns. One area in which we would like clarification is regarding the “analysis of risk to the BES” or the system.   Does this analysis need to be performed and documented on a per patch basis? On a vulnerability basis? Can entities create processes for system analysis with standard categories that have appropriate timeframes associated with them?

Southern is also concerned with the "Secure Configuration" which could end up being a vast number of methods on various systems and is no longer bound to five discrete software change categories. Proving proof of change management on every change to any kind of "method" throughout CIP-005 and CIP-007 will be challenging if not impossible.

For Part R3.6 Southern would like clarification stating that existing mitigations may be sufficient for the risk of a particular vulnerability and the entity may not have any further analysis or mitigation required because of these existing mitigations.   In other words, past applied compensating controls may also cover many future vulnerabilities. It needs to be clarified that this situation is either A) not an applicable vulnerability in part 3.5, or B) it is, but nothing FURTHER needs to be done in 3.6. Southern prefers option A.

Likes 0

Dislikes 0

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group

Answer No

Document Name

Comment

Generally, it is not clear why the proposal is to move away from the concept of an undefined baseline configuration to the “Secure Configuration.” The new requirements in Parts 3.5 and 3.6 of CIP-010-4 are less prescriptive than what is being replaced from CIP-007, and appears to allow a more subjective approach for determining the timeline and periodicity for identifying vulnerabilities. The SSRG recommends the Standard Drafting Team review the draft to ensure its objectives are being met.

Specific to “b” - this change will increase the number of Cyber Asset attributes that need to be tracked from what was previously considered baseline, and will heighten the compliance risk for change control. For instance, when a new generic account is added to a Cyber Asset (common operator account) the current requirements provide for identification and inventory. The proposed requirement makes a new generic account part of the Secure Configuration and will require the CIP-010-4 Part 1.1 change control processes. Currently, following the CIP-010-2 change control process for a new generic account is a best practice but not a violation. This is just one example where the proposal is not backwards compatible. Creating the new Secure Configuration definition and tying the definition to CIP-010-4 will significantly increase compliance work and introduces auditor discretion.

Specific to “c” the SSRG doesn’t think it matters whether CIP-007 or CIP-010 houses the requriements. However, the real issue is the uneccesary documentation changes that will be required to move the language; therefore, the drafting team may consider whether moving the requirements to CIP-010 is the most efficient means to address the issues.

Likes 0

Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA

Answer	No
Document Name	

Comment

Moving to a security objective approach implies for a need for a cyber-security plan which considers the risk and appropriate mitigation and controls to meet the objective.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	No
Document Name	

Comment

The introduction of the new term Secure Configuration and its role is unclear. The proposed security objective throughout the Requirements in CIP-010 does not offer any clarity. For example removing the 35 day requirement for patching leaves it open to an auditor's interpretation of what they think is appropriate. Also, in CIP-10 R3, 3.5 the following sentence needs clarification and guidance: "The process of Part 3.5 shall include the periodicity for identifying software vulnerabilities based on the risk to BES reliability and the impact rating of the applicable system(s)."

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	

Comment

Regarding subquestion B, Tri-State requests clarification on the control change process outlined in CIP-010 R1.1, specifically the language in R1.1.2 "could be impacted by the change." Is the intention of this requirement for each entity to make a determination of what could be impacted, or is the intention that each of the Secure Configuration components throughout these changes in CIP-005, CIP-007, and CIP-010 are the universe that must be considered?

Additionally, in CIP-010 R1.2.1 would like clarification of what specifically is included as "required" in the language "to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected"

Regarding subquestion B and the components of Secure Configuration, Tri-State requests that CIP-007 R3.1. and R3.2 are updated with language to require these sub-parts only if the system is capable.

CIP-007 R3.1 recommended updated language reads: "Deploy method(s) per system capability to deter, detect, or prevent malicious code"

R3.2 recommended updated language reads: "Mitigate the threat of detected malicious code, per system capability."

Regarding subquestion C, Tri-State recomends adding "or" after each bullet (similar to recommendations in Question 14). This language will clarify the ability to choose from the list.

CIP-010 R3.5 recommended updated language reads:

• Vulnerability database monitoring; or

• Patch source monitoring; or

• Vulnerability scanning; or

• Other method(s) to identify software vulnerabilities.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI’s concerns over the proposed changes to CIP-010 align with our comments and concerns as described for Questions 12.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No

Document Name	

Comment

Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

The parts of Requirement R1 could be improved by putting the parts in sequence with actual change control (eg, implement in test, security controls testing, approve for production, etc.). As written the requirement is difficult to follow. The last statement in Part 1.1 should be guidance. It is not written as an objective requirement.

The last statement in Parts 2.1 and 2.2 should be guidance. They are not written as an objective requirement.

Requirement R3 is a good change over the current approach to patching. However, these changes may require significant significant capital investment and process changes. Requirement Part 3.6 should include provisions for changing a mitigation plan, similar to the current requirement in CIP-007 Requireemnt R2. This would allow entities to address changes in their timeline without the risk of a violation.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

No, NRG does not agree that adding the security objectives throughout the Requirements in CIP-010 adds clarity to the reason the requirement exists because: The changes to CIP-010 change the understood intent of the standard from Change Control to a hybrid objective. A recommendation would be to change the standard to “Vulnerability Management” and realign the requirements with the new objective.

No NRG does not agree with the proposal to modify the referenced baseline configuration from CIP-010-3 R1 Part 1.1 to a ‘Secure Configuration’ which is made up of the implemented controls that fulfill requirements within CIP-005 and CIP-007 and that this set of controls supports managing change under CIP-010 R1 Part 1.1 NRG asserts that the requirement changes while reducing overall compliance burden, introduce a new “spaghetti” requirement. NRG recommends that a specific list of Secure Configuration, even as an addendum, would be helpful.

No, NRG does not agree with the proposal to modify the current CIP-007 R2 requirements and move them to CIP-010 R3 and does not believe that the software vulnerability management found within this set of requirements fits logically within the security objective of CIP-010 R3 “to mitigate the risk posed by system vulnerabilities" because the intent of CIP-007 patch management requirements were readily understood by the industry, while developing a risk based system is left to the interpretation of each Registered Entity. The result is going to be a large disparity in patching cycles between entities and even within the same entity. This will make auditing & benchmarking more difficult and could lead to industry difficulty with implementation of standards change.

No, NRG does not agree that the proposal of CIP-010 R3 Parts 3.5 and 3.6 to replace the current CIP-007 R2 Parts 2.1 – 2.4 offers the additional flexibility needed when implementing virtualized systems that can be dormant for a period, and for which security patches have become available because in relation to virtualized systems, NRG asserts that the proposed requirements do offer flexibility. However, there is no prescriptive criteria to manage the duration of dormant periods.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

While we agree with adding the security objective to the requirements it appears that a security objective was not added to R4.

We believe that the relocation of CIP-007 R2 to CIP-010 R3 makes much more sense and allows for Entities to finally address vulnerabilities as part of compliance and not just potentially wasted effort on patches which are only a component of vulnerability management. In addition, Entities now can get compliance credit for addressing vulnerabilities when announced rather than waiting for patches which may lag the vulnerability announcement by months. However, the concept of revising a vulnerability mitigation plan in CIP-007 R2.4 does not appear to have been ported to the CIP-010 R3 modifications.

While we appreciate the SDT trying to revise CIP-010 R1 for the better, it is currently a chicken and the egg requirement. The requirement states, "Control change to the Secure Configuration" and "Prior to the change determine required cyber security controls in the Secure Configuration that could be impacted by the change." So, if we are to control change to the Secure Configuration then we need to know what will change and yet we are to take an educated guess as to what in the Secure Configuration COULD be changed. Also, the question is prior to what change? The previous requirement was changes to the Configuration Baseline. We would recommend that the impetus for change management should still be defined as a change to Operating System, or firmware where not OS exists, change to software versions, and the application of all patches not just security patches. Changes to logical network accessible ports should be dropped from the list of items that prompt a change given the modified CIP-007 R1.1 controls. If necessary, these change triggers could be defined as Configuration Change. However we believe the concept of Configuration Baseline can be dropped in favor of a Secure Configuration. Tracking the Configuration Baseline is no longer required when the modifications to CIP-007 R2 address the security objective of unmanaged software. Also, it is unclear when CIP-010 R1.3 would be triggered if the impetus is a change the Secure Configuration and not a Configuration Change. If an entity implemented application whitelisting for CIP-007 R2.1 then would CIP-010 R1.3 ever be triggered? The impetus is a change that deviates from the Secure Configuration. If application whitelisting remains implemented when the OS, firmware, software (or patch) is installed or updated then did the Secure Configuration ever change? If not, then an entity doesn't have to perform either of the verification tasks. Therefore, the impetus for any CIP-010 R1 change should be a Configuration Change like before, but without tracking the Configuration Baseline.

We have concerns regarding the monitoring of the implemented Secure Configuration in CIP-010 R2. First, we have implemented Device Specific Test Plans for many types of Cyber Assets for the current CIP-010 R1. While many aspects of the Secure Configuration can be monitored through configuration monitoring, many still require the inspection through configuration auditing which is more time consuming for personnel. In addition, unauthorized change to the Secure Configuration could be considered a system vulnerability and should potentially be managed under that security

objective. If it is managed under R3 then it should be only performed if monitoring of a Secure Configuration property has not occurred in X amount of time. This is because many of the Secure Configuration properties would be inspected throughout the year as part of the change management process.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro’s view is that the inclusion of serial port configuration in the Secure Configuration is too broad and may not be manageable relative to the risk posed. Also, it seems unclear whether USB ports would be considered in scope.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE does not agree CIP-010 needs to be changed with regards to virtual systems. Virtualized systems should be baselined just like physical systems as they are currently done. Texas RE has not seen issues specifically caused by virtualization using the current approach.	
Likes 0	
Dislikes 0	
Response	

16. Provide any additional comments for the SDT to consider, if desired.

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	
Document Name	

Comment

Clarification for the CIP-010-4 R1.2 term "models" would be valuable. This is an ambiguous term that in current standards provides confusion for what will satisfy expectations. We see this as possible via formalizing the term with definition, stating more clear aspects, or including specific guidance in the supporting documentation of the standard.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	
Document Name	

Comment

First, MISO would like to thank the SDT for their efforts in drafting these revisions. Revising existing CIP Standards is a difficult task and MISO appreciates the quality of the proposed changes and the effort put forth by the Team. MISO is encouraged by the work to modernize the standards and recognize that many modern software and hardware configurations are capable of safely and securely separating BES and non-BES workloads on the same physical hardware. The move to LIZ that is not focused on a subnet centric design is welcome. The changes to a risk based approach to patching instead of a hard time limit is also encouraging, however guidance will need to be provided on what will be required when audited to ensure that the risk criteria and decisions made around patching are appropriate and compliant.

The proposals do raise some questions with MISO around data protections for data in transit, as well as the definition of "secure configuration" and what may need to be demonstrated for that requirement.

The proposed changes do not yet tackle in any way the use of "cloud" or off-prem providers who would have continual management connectivity into the environment for CIP computational or storage workloads. They also do not yet address handling certain types of CIP data using Cloud storage providers.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company

Answer	
Document Name	

Comment

Overall, we support changing from prescriptive-based requirements to objective-based requirements and most of the concepts presented to help clarify virtualization in the CIP environment. However, aside from the concerns mentioned throughout, we do have some concerns on how the updated requirements will be audited. Specifically, how will the auditors apply the requirements to entities that have no virtualization or entities that have their virtual environments segmented (i.e. one virtual environment for high impact BES Cyber Systems, one virtual environment for associated high impact EACs, one virtual environment for associated high impact PACS, etc.)?

We are also in support of EEI comments.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	
Document Name	

Comment

In the development of NV Energy comments, we have struggled with trying to find some middle ground that acknowledges the hard work and laudable efforts made by the SDT, unfortunately, the structure of the comment format did not lend itself to such comments.

Nevertheless, NV Energy cannot support the level of change being proposed at this time, due to the recognition that virtualization remains a small piece implemented within the industry, and will continue as such for the foreseeable future. This has led us to the conclusion that SDT efforts need to focus more on the how virtualization might be effectively integrated into BES Cyber Systems, under the current standards, rather than trying to solve all these issues at an early stage of industry adoption.

NV Energy does not support the overly broad and sweeping change proposed by the SDT because it is premature. While there are aspects of what the SDT is considering that may have future benefit and utility, employing those changes at this time would prove to be too disruptive to existing efforts by the industry. Furthermore, there is limited acceptance of virtualized networks within the industry and efforts to try and tailor the current body of standards to accommodate this emerging security solution is likely to create needless security concerns. Instead the SDT should work toward addressing the more immediate needs of the industry such as clarifying how the security and management of BES Cyber Systems can be accomplished in a virtualized environment using the existing body of standards, as currently approved. We further believe that the level of change being considered by the SDT would be better addressed through a separate initiative spanning several years to allow more engagement by the industry.

NV Energy also notes that while the SDT has offered up some very interesting ideas to address virtualization within BES Cyber Systems, many Responsible Entities still feel there is a lack of overall clarity necessary to address the design, control, and protection of these systems in a virtualized environment.

NV Energy’s last concern centers on the auditability of the proposed approach. While the security objective-based approach does provide a friendlier environment for virtualization, we are concerned that from an audit perspective this approach may prove to be very difficult for Responsible Entities and auditors to demonstrate compliance leading to interpretations and judgements that could impact the security of BES Cyber Systems, while placing into question whether the proposed solution can be effective and consistently audited.

Likes 0

Dislikes 0

Response

Michael Johnson - Consultant - NA - Not Applicable - NA - Not Applicable

Answer

Document Name

Comment

None

Likes 0

Dislikes 0

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer

Document Name

Comment

CenterPoint Energy supports EEI's comments and approach for the next steps to address virtualization. It is important to highlight that these revisions were not mandated by a FERC order. Furthermore, entities with virtual environments are already complying with the existing CIP standards. In order to address virtualization and other emerging technologies, CenterPoint recommends that the SDT focus its efforts in transferring these concepts to Implementation Guidance or through a separate inititive to allow more engagement by the industry

While the proposed revisions offer some flexibility for implementation, CenterPoint Energy is not in favor of the level of changes being proposed by the STD team at this time. The large fundamental changes proposed in this draft may introduce potential unintended consequences and challenges with auditability at a time when the industry is affirming compliance with the current version of the CIP standards.

If the SDT continues to proceed with these revisions, CenterPoint Energy recommends addressing the items commented above and conducting implementation pilots to surface implementation challenges, similar to what was done with the CIPv5 pilots.

Likes 0

Dislikes 0

Response

Susan Sosbe - Wabash Valley Power Association - 3

Answer

Document Name	
Comment	
Wabash Valley thanks the SDT for the hard work to meet a difficult and evolving challenge. As this appears to be a total redo of large parts of the standard, the SDT should consider that techniques similar to those used in the implementation of version 5 of the standard may be required to fully flesh out the revisions, preferably prior to final approval of the new standard.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	
Document Name	
Comment	
We urge the drafting team to implement this in stages and consider the EACS/EAMS and PACS/PAMS changes initially. These changes will have the least operational impact and the greatest security benefits. Introduction of secured configuration and CIP-005 changes should be transitioned over time to reduce operational risk and impact.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	
Document Name	
Comment	
Westar | Kansas City Power & Light Company incorporate by reference Edison Electric Institute’s response to Question 16.	
Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	
Document Name	

Comment

Seattle City Light recognizes the complex and difficult job the SDT had in drafting the proposed virtualization standards, and applauds the persistence and creativity shown in crafting the present proposal. We appreciate these efforts. Project 2016-02 provides best practices for security standards that strive to stay ahead of adversaries' efforts. The Project is groundbreaking and is the first step toward the next level of the best practices in security standards. We see this effort to date as significant progress.

Importantly, refining and implementing the virtualization standards will be a challenge for NERC and industry. Seattle suggests the following as general principles that might guide futher development of the the proposed virtualization changes:

We strongly support for direction of proposed changes, as very promising and necessary to accommodate technological change and increasing theats

That said, the changes proposed are more far-reaching than expected, likely have many unintended consequences, are in some areas complex and largely untried, and in other cases expand the CIP scope to address new vulnerabilities introduced by virtualization

Therefore, Seattle recommends consideration of a parallel "virtualization overlay" approach, in which the Standards are revised such that the existing definitions and existing requirements are retained, but the proposed new definitions and new requirements are also an option. An entity must identify which approach they choose, on a cyber-system by cyber-system basis. This approach ensures backwards compatibility, minimizes the impact on entities that do not employ virtual technology, and yet frees other entities to pursue the possibilities of virtualization.

The overlay approach might by designed to sunset after a time, or be reassessed at a certain point based on lessons learned. It might be considered as a sort of CIP version of the PRC-005-2 to PRC-005-6 trransition.

Expansion of CIP scope to address new vulnerabilities associated with virtualization should be restricted only to virtualized BCS. These changes should not increase scope for non-virtualized BCS.

Seattle strongly urges that NERC sponsor a pilot project with volunteer utilities, as happened with CIP v5 changes be utilized with virtualization.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	
Document Name	

Comment

Exelon appreciates the work and time that the SDT as put into this effort. We do see value in moving toward security objective-based requirements and being less technology dependent. We agree with many of the ideas, including splitting out lower risk monitoring from access control. However, we believe that the sweeping changings as now proposed are overly broad, including foundational definition changes, and these will radically impact current CIP programs.

As far as virtualization, Exelon has successfully implemented virtualization using a “conservative” architecture approach, while maintaining compliance with the current CIP requirements. We do see the potential of architecting virtualization and other technologies in new ways in the future to increase reliability and security while decreasing cost. CIP Standard changes to address new technologies and architectures are needed but are more appropriately addressed in a separate longer-term and comprehensive CIP version change effort. That effort should also take into consideration many other factors beyond virtualization that have surfaced since CIP V5 to improve the CIP Standards overall. Such an effort we could support.

We would prefer to see the current SDT address the more immediate needs of the industry such as clarifying how the security and management of BES Cyber Systems can be accomplished in a virtualized environment using the existing body of standards, as currently approved.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6, Group Name Lakeland CIP

Answer	
Document Name	

Comment

Lakeland Electric supports the comments provided by the American Public Power Association (APPA). We appreciate the work of the Standards Drafting Team in addressing the changing technology needs of industry.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI

Answer	
Document Name	

Comment

In general AECI agrees with the revisions to address virtualization for the follow reasons:

*Not materially changing non-virtualization compliance

* Providing the explicit ability to demonstrate compliance while using virtualization

* Allows CIP compliance program concepts to mature as the BCA term is retired

Additionally AECI raises an additional concern that the standards may not adequately address the “shared responsibility” aspect of using cloud computing resources, such as Azure or AWS. This was a topic of discussion at a recent NERC CIPC meeting, FedRAMP requirements were explained as possibly being a good model for addressing the shared responsibility issues. (https://www.fedramp.gov/)

Likes 0

Dislikes 0

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer

Document Name

Comment

Thank you for the opportunity to comment

Likes 0

Dislikes 0

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer

Document Name

Comment

We urge the drafting team to implement this in stages and consider the EACS/EAMS and PACS/PAMS changes initially. These changes will have the least operational impact and the greatest security benefits. Introduction of secured configuration and CIP-005 changes should be transitioned over time to reduce operational risk and impact.

Likes 0

Dislikes 0

Response

Stephanie Burns - International Transmission Company Holdings Corporation - 1 - MRO,RF

Answer

Document Name

Comment

ITC is in agreement with the comments submitted by EEI:

"In the development of EEI comments, we have struggled with trying to find some middle ground that acknowledges the hard work and laudable efforts made by the SDT, unfortunately, the structure of the comment format did not lend itself to such comments. Additionally, while EEI's comments may be viewed as largely negative; we recognize that many of the ideas being developed by the SDT have significant future merit. Nevertheless, we cannot support the level of change being proffered at this time due to the recognition that virtualization remains a niche effort within the industry and will continue as such for the foreseeable future. This has led us to the conclusion that SDT efforts need to focus more on the how virtualization might be effectively integrated into BES Cyber Systems, under the current standards, rather than trying to solve all these issues at an early stage of industry adoption.

EEI does not support the overly broad and sweeping change proposed by the SDT because it is premature. While there are aspects of what the SDT is considering that may have future benefit and utility, employing those changes at this time would prove to be too disruptive to existing efforts by the industry. Furthermore, there is limited acceptance of virtualized networks within the industry and efforts to try and tailor the current body of standards to accommodate this emerging security solution is likely to create needless security concerns. Instead the SDT should work toward addressing the more immediate needs of the industry such as clarifying how the security and management of BES Cyber Systems can be accomplished in a virtualized environment using the existing body of standards, as currently approved. We further believe that the level of change being considered by the SDT would be better addressed through a separate initiative spanning several years to allow more engagement by the industry.

EEI also notes that while the SDT has offered up some very interesting ideas to address virtualization within BES Cyber Systems, many Responsible Entities still feel there is a lack of overall clarity necessary to address the design, control, and protection of these systems in a virtualized environment.

EEI's last concern centers on the auditability of the proposed approach. While the security objective-based approach does provide a friendlier environment for virtualization, we are concerned that from an audit perspective this approach may prove to be very difficult for Responsible Entities and auditors to demonstrate compliance leading to interpretations and judgements that could impact the security of BES Cyber Systems, while placing into question whether the proposed solution can be effective and consistently audited."

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	
Document Name	

Comment

Be consistent with the use of "such as", "e.g.", and other illustrative phrases. While the changes proposed are a definite improvement to the standards, there will be a significant cost to implement these changes. These include revisions to change management systems, inventory systems, and other supporting tools used for audit evidence. As the drafting team looks at the implementation plan for these changes, consider how to allow entities to absorb these costs over time.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 1,3,5,6, Group Name LES

Answer	

Document Name	
Comment	
Overall, LES supports the direction of this project.	
Likes 0	
Dislikes 0	
Response	
Lana Smith - San Miguel Electric Cooperative, Inc. - 5	
Answer	
Document Name	
Comment	
SMEC appreciates the efforts of the SDT. However, we disagree with the approach of substantial changes to numerous standards and definitions in order to address virtualization. SMEC suggests that a better solution would be a new CIP standard that applies to virtualized CIP Systems or to provide clear implementation guidance on protecting BES Cyber Systems within virtualized environments under the existing framework and standards already in place. SMEC is concerned that this magnitude of change to the CIP standards when many entities have not yet been audited for CIP v5 would be too disruptive to non-virtualization compliance.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 1,3,5,6	
Answer	
Document Name	
Comment	
NYPA is concerned given the proposed expansion of the Secure Configuration concept, as this has the potential to significantly increase the scope of identified BES Cyber System Information, thereby adding administrative overhead to track this, and the creation of numerous new BCSI documents / repositories which poses a risk.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,2,3,4,5,6,7,8,9,10 - MRO	

Answer	
Document Name	
Comment	
Please see MRO NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
Support MRO NSRF additional comments	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP requests that SDT provides technical guidelines and examples for each requirement that has been modified/added.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	
Document Name	

Comment

LCRA would like to thank the drafting team for the time and effort invested in creating these proposed changes.

Likes 0

Dislikes 0

Response

Robert Ganley - Long Island Power Authority - 1

Answer

Document Name

Comment

General overall comment, the newly proposed definitions need to be re-evaluated, clarified, and agreed before the standards and requirements can be fully understood.

Likes 0

Dislikes 0

Response

Don Schmit - Nebraska Public Power District - 1,3,5

Answer

Document Name

Comment

In NPPD’s opinion the proposed changes are too wide sweeping and transformational in nature without adequately addressing the more immediate need to clarify how the security and management of CIP systems in virtualized environments (or any new emerging technology) can be accomplished. Changes of this magnitude should be accomplished under a separate initiative with an adequate timeframe that allows proper engagement with industry to develop an approach to CIP compliance that can better adjust to changes in technology and risk environments.

NPPD does encourage the drafting team to develop industry guidance for virtualization. However, as stated, the industry should have a focused (not rushed) effort to evaluate what is needed within the CIP Standards as changing or new technology emerge.

Continual overhaul of the NERC Standards means increased risk to the Bulk Power System, as resources are siphoned off to align entity programs to continual change to the Standards. NPPD encourages the drafting team to issue guidance to the industry on virtualization and, if necessary, develop a single separate NERC Standard for Virtualization. However, a larger overall solution must be attained for new/emerging technologies and risk without the continual overhaul of the CIP suite of Standards

Likes 0

Dislikes 0

Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	
Document Name	AZPS Comments - Question 16.docx
Comment	
Please see the attached document.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
IESO agrees that the changes only needed to “backwards compatible” from a controls/ program perspective. IESO agrees that, as a primary consideration, the proposed changes do not have to be “backwards compatible” at the device level	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	
Document Name	
Comment	
MEC appreciates all the thoughtful hard work the SDT has put into this effort. That said, the changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Some entities have not had the chance for an audit on the last round of changes. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective. MEC has compliantly implemented virtual servers within the existing CIP standards structure. We have been audited on CIP-005 and CIP-007 as well as CIP-004 and CIP-006. We have self-certified CIP-002, -003, -008 and -011. And are preparing evidence for an audit on CIP-009 and CIP-010 in 2019 and have not identified issues.	

It is not clear how this magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the “how to comply” with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	

Comment
Xcel Energy fully supports the comments submitted by the MRO NSRF and Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Daniel Valle - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6 - NPCC	
Answer	
Document Name	

Comment
Moving to a security objective approach implies for a need for a cyber-security plan which considers the risk and appropriate mitigation and controls to meet the objective. In the development of our comments, we have struggled with trying to find some middle ground that acknowledges the hard work and laudable efforts made by the SDT, unfortunately, the structure of the comment format did not lend itself to such comments. Additionally, while our comments may be viewed as largely negative; we recognize that many of the ideas being developed by the SDT have significant future merit. Nevertheless, we cannot support the level of change being proffered at this time due to the recognition that virtualization remains a niche effort within the industry and will continue as such for the foreseeable future. This has led us to the conclusion that SDT efforts need to focus more on the how virtualization might be effectively integrated into BES Cyber Systems, under the current standards, rather than trying to solve all these issues at an early stage of industry adoption. We do not support the overly broad and sweeping change proposed by the SDT because it is premature. While there are aspects of what the SDT is considering that may have future benefit and utility, employing those changes at this time would prove to be too disruptive to existing efforts by the industry. Furthermore, there is limited acceptance of virtualized networks within the industry and efforts to try and tailor the current body of standards to accommodate this emerging security solution is likely to create needless security concerns. Instead the SDT should work toward addressing the more immediate needs of the industry such as clarifying how the security and management of BES Cyber Systems can be accomplished in a virtualized

environment using the existing body of standards, as currently approved. We further believe that the level of change being considered by the SDT would be better addressed through a separate initiative spanning several years to allow more engagement by the industry.

We also note that while the SDT has offered up some very interesting ideas to address virtualization within BES Cyber Systems, many Responsible Entities still feel there is a lack of overall clarity necessary to address the design, control, and protection of these systems in a virtualized environment.

Our last concern centers on the auditability of the proposed approach. While the security objective-based approach does provide a friendlier environment for virtualization, we are concerned that from an audit perspective this approach may prove to be very difficult for Responsible Entities and auditors to demonstrate compliance leading to interpretations and judgements that could impact the security of BES Cyber Systems, while placing into question whether the proposed solution can be effective and consistently audited.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	
Document Name	

Comment

Each change to a standard creates additional work for an entity to evaluate its processes, revise where appropriate, implement the changes, and retrain employees, which is not cost-effective. The proposed changes to the CIP standards will have significant impacts on entities and will require substantial resources to implement. The proposed changes go beyond simply updating technology and/or documentation; they constitute a culture shift comparable to the CIP v5 transition. Entities must implement processes to achieve an understanding of new terms, buy in to their use, and change their the culture to employ new terms. Entities must be provided sufficient time to determine the effects of the revised requirements and definitions, develop adequate processes, and train personnel appropriately in order to implement quality practices that improve BES reliability. Reclamation recommends a minimum of 24 months for all entities to implement the proposed changes, with an additional 18 months for entities that use virtualization to achieve compliance.

Where possible, Reclamation recommends the SDT use the following existing industry terms:

Intrusion Detection and Prevention System (IDPS) – Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Prevention System(s) (IPS) – System(s) that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

Intrusion Detection Systems (IDS) – System(s) that detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.

Enclave – A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

Enclave Boundary – Point at which an enclave’s internal network service layer connects to an external network’s service layer, i.e., to another enclave or to a wide area network (WAN).

Reclamation recommends adding the following new terms to the NERC Glossary of Terms:

Physical Access Control and Monitoring System (PACMS) – Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Electronic Security Enclave (ESE) – One or more Cyber Assets logically connected by one or more internal communication control(s) of a single authorizing security policy for BES Cyber Systems and Protected Cyber Systems. The logically connected Cyber Assets may be structured by physical proximity or by function, independent of location.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1,3,5,6, Group Name Manitoba Hydro

Answer	
Document Name	

Comment

Given that as long as the virtual CIP Cyber Assets are identified appropriately, most of existing CIP V5 requirements worked with these virtual CIP Cyber Assets very well based on previously NERC and MRO's advices regarding virtualization. We disagree with these significant directional changes that are only for sufficing a very small percentage of the virtual devices while ignoring the fact that the majority of physical devices are working smoothly for the existing requirements. The major issue for the existing CIP V5 requirements is that the virtual Cyber Assets are not explicitly required in the current standard language. After revising the Cyber Asset definition to include the virtual devices, most of the compliance issues will be resolved. SDT's strategy for the virtualization should focus on developing few additional requirements that only apply to the virtual CIP Cyber Assets if the existing requirements cannot be addressed in the virtual environment. Resulting from we suggested strategy, it would be beneficial for all registered entities as follows:

•   For the registered entities that have no any virtual CIP Cyber Assets, they may not need to do anything.

•   For the registered entities that have some virtual CIP Cyber Assets, they would only need to address the additional requirements for their virtual CIP Cyber Assets unless they could resolve them using the existing requirements.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	
Document Name	

Comment

Overall, the NSRF does not agree with the direction of this Project. There are other ways of applying and testing of new directions without doing a complete overhaul of the existing standards and associated overhaul of industry's programs. Originally, there was the Version 5 Transition Advisory

Group, made up of 6 Entities to test our current suite of Standards. There are also multiple registered groups who can write and submit to NERC, Implementation Guidance for ERO deference. Any radical change to the CIP Standards should be practiced and tested BEFORE any Standard is recommended for change. The NSRF also believes that there are Entities who are currently compliant (via an audit) by incorporating virtualization practices under our current set of Standards. All Standards are written to “what to do” not how to incorporate a certain or new technology. The NSRF has attempted to answer the SDT questions but still does not agree with this Project. Here are some specific examples of what a small change to a Standard will do to the industry.

The MRO NSRF remains concerned with the subjectivity this will bring to meeting compliance. Auditors come from varying backgrounds and while one auditor may not have an issue with an entity’s risk based assessment, the next auditor may. This may even be true with an entity. The industry experienced this with the CIP-002 RBAM and then was later asked to change to a more prescriptive set of requirements.

We do not agree with the SDT direction at this time. The NSRF feels that the proposed changes are too wide sweeping and transformational in nature without adequately addressing the more immediate need to clarify how the security and management of CIP systems in virtualized environments can be accomplished. Changes of this magnitude should be accomplished under a separate initiative with an adequate multi-year timeframe that allows proper engagement with industry to develop a new approach to CIP compliance that can better adjust to changes in technology and risk environments.

In the meantime, we recommend that the SDT narrow their focus back to the issue at hand which should be clarified standards and guidance for systems that exist within a virtualized environment. One possible recommendation would be to look at the development of a new CIP Standard that solely addresses the base level controls, security and configuration requirements for virtualized CIP systems and modify other existing CIP Standards and Requirements to exempt virtualized systems when applicable. Taking this approach would provide the clarity that is needed today for entities currently utilizing or planning to utilize virtualization with their CIP systems without requiring yet another complete NERC CIP program overhaul

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3,5

Answer	
Document Name	

Comment

AEP is concerned with the addition of veiled requirements to conduct "risk" analyses in proposed CIP-010-4 R3 Parts 3.5 and 3.6. Our understanding is that the "impact to the BES" is in fact the risk based on the equation used when the bright lines were established: Risk equals Threat times Vulverability times Impact, where Impact is the only variable and Threat and Vulnerability are defined as being equal to one. Also, sufficiency criteria for the risk analysis have not been established so this will likely become another source of contention when compliance is assessed. The work involved with assessing and documenting the "risk" for every component of every high and medium impact BCS across the BES will be enormous. AEP believes there should be an alternative to the "risk" analysis, stated in the Requirement, such as checking for patches and implementing/mitigating on the current 35 day cycles.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

PacifiCorp's approach to this informal comment period was to provide the SDT with constructive feedback related to the proposed revisions to the terms, standards and concepts presented. With that said, PacifiCorp has additional comments and concerns that will be addressed here.

PacifiCorp does not support the overly broad and sweeping change proposed by the SDT, feeling that the effort is premature. While there are aspects of what the SDT is considering that may have future benefit and utility, employing those changes at this time would prove to be too disruptive to existing efforts by the industry.

PacifiCorp's primary concern centers on the auditability of the proposed approach. While the security objective-based approach does provide a friendlier environment for virtualization, we are concerned that from an audit perspective this approach may prove to be very difficult for Responsible Entities and auditors to demonstrate compliance leading to interpretations and judgements that could impact the security of BES Cyber Systems, while placing into question whether the proposed solution can be effective and consistently audited.

The changes being proposed within the body of revised, retired and new definitions and the impact on the applicable systems represents another overhaul of the CIP standards and associated Responsible Entity compliance programs too soon after the last one. Other revisions, such as CIP-003-7 sections 2, 3 and 5 have yet to become effective.

It is not clear how the magnitude of changes will create a corresponding improvement to reliability and security. Perhaps the "how to comply" with the existing standards when virtualization is involved could best be addressed using other tools such as ERO-endorsed implementation guidance or readiness reviews for the segment of Responsible Entities who are operating or plan to operate with virtualization.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1,3,5,6

Answer	
Document Name	

Comment
None

Likes 0	
Dislikes 0	

Response
Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment
It appears most of these changes are not specific to virtualization as the project indicates. Rather, the changes indicate a shift in the CIP Reliability Standards. As the industry recently implemented version 5 of the CIP standards, this puts an additional burden to comply with the proposed changes. Texas RE is not convinced a shift in the CIP standards is necessary. If the SDT feels it is necessary, the entire body of CIP Reliability Standards should be evaluated. Texas RE requests the SDT provide justification for the proposed changes by the V5 TAG, since that is what is referenced in the June 1, 2016 Standards Authorization Request.

Likes 0	
Dislikes 0	

Response
Russell Noble - Cowlitz County PUD - 3,5

Answer	
Document Name	

Comment
Cowlitz supports APPA comment. Futher, we believe the standards must evolve to allow virtualization application.

Likes 0	
Dislikes 0	

Response

Nathaniel Clague - Portland General Electric Co. - 1,3,5,6

Answer	
Document Name	

Comment

PGE supports the direction that the drafting team is taking. The CIP standards framework should not serve to limit the use of new technologies that meet the security objectives and this poposed set of standards makes great strides in accomplishing that outcome. PGE encourages the continued engagement of FERC and the ERO enterprise to develop and document consistent approaches to implementing and auditing these new standards.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	
Document Name	

Comment

A concept not address in the concepts in a virtual TCA. So, in a virtualized environment if an entity spins up a new virtual machine, but the wrong base image was used, and it is deactivated within 30 days of creation is it now a TCA?

The creation of virtual machines should be addressed. Is cloning from a base virtual machine in the environment acceptable since it already has all the security controls applied? What about when a new base image needs to be created? Must it be created in a test bed first then moved to production. However, typically the security controls of policies and targets for systems managing backups, anti-malware, logging and other may be different. So, can a new virtual machine have only some security controls in place if they are applied in a reasonable time frame when connected to production? This is also a problem for new physical equipment as well.

As pointed out in another comment, some of the V5TAG items in the Standards Authorization Request are not addressed by these proposed revisions.

We appreciate the SDT's effort on this issue. While our comments may appear negative, they are only pointing out the problems and concerns we have identified. The revisions to CIP-010 R1, R3, and CIP-007 R2 are a step in the right direction when it comes to the current pains of CIP compliance. If the SDT focused on those changes and the V5TAG issues remaining, then we might be able to get to a better set of requirements. However, some of the overly broad and sweeping changes to both defined terms and requirements may be more than the industry can digest at this time. The SDT needs to focus on how virtualization fits into the current requirements. Furthermore, we like the idea of meeting security objectives with a selection of one or more protection elements to achieve the objective. This is much better than overly prescriptive controls that do not always fit. We prefer examining this path and not the other fork in the road with overly prescriptive requirements trying to tie an industry to best practices as they exist today. If the SDT wanted to future proof the requirements then the requirements should be reworked with the stated security objective and let the Entity develop a program or plan to address that security objective and include the identification of the controls, and potentially a means to measure control effectiveness. An Entity would have to maintain an effectiveness greater than X to stay compliant. Or a third-party review like CIP-014 could be implemented. The threat remains relatively unchanged over the years; someone with malicious intent causing adverse impact to one or more BES Facilities. However, the attack vectors and protections against those attack vectors continue to change. Unless Entities can be allowed to develop their

own programs to identify the attach vectors and protections, then the requirements will always lag the existing threat landscape when new vectors are identified.	
Likes 0	
Dislikes 0	
Response	
James Grimshaw - CPS Energy - 1,3,5	
Answer	
Document Name	
Comment	
Because the new standards would be moving away from a prescriptive approach into a more fluid one, CPS Energy will need to make sure we have in writing our reasoning behind our thresholds/our procedures in general. Our procedures will need to have this information for us to provide as evidence to the auditors. There should be another means for CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
In review, NRG asserts that the modifications presented by the SDT represent a drastic shift in philosophy of the standards that are significantly more substantial than an introduction of virtualuzation defintion, akin to the shift from v3 to v5. NRG applauds the SDT in the attempt at shifting the focus to enourage security. However, an ambiguous approach could lead to a wide disparity in implementation between Registered Entities. This could `make the auditing of CIP much more subjective and also industry inderstanding much more subjective also. The shift raises concerns of reintroducing difficulties from previous versions of the standards, i.e. risk-based methodology for CIP-002 and "spaghetti" requirements.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	

Document Name	
Comment	
Be consistent with the use of “such as,”, “e.g.,” and other illustrative phrases. While the changes proposed are a definite improvement to the standards, there will be a significant cost to implement these changes. These include revisions to change management systems, inventory systems, and other supporting tools used for audit evidence. As the drafting team looks at the implementation plan for these changes, consider how to allow entities to absorb these costs over time.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	
Document Name	
Comment	
Ameren supports and agrees with EEI comments (MS_2016-02_CIP_Virtualization_EEI Comments final.pdf)	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	
Document Name	
Comment	
Because the new standards would be moving away from a prescriptive approach into a more fluid one, CPS Energy will need to make sure we have in writing our reasoning behind our thresholds/our procedures in general. Our procedures will need to have this information for us to provide as evidence to the auditors. There should be another means for CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	
Document Name	

Comment

In the development of EEI comments, members struggled with trying to find some middle ground that acknowledges the hard work and laudable efforts made by the SDT as most members identified with the progressive, forward thinking of several proposed concepts. However, EEI members agree that many of the ideas being developed by the SDT have merit.

As noted in question 1, these comments do not represent a consensus, but we offer them for the SDT to consider. At this time, the EEI members who participated in the development of these comments do not support the level of change being proffered due to the recognition that virtualization remains limited in its adoption within the industry and is expected to continue as such for the foreseeable future. This is not to diminish the fact that in many sectors outside of the electric utility industry virtualization is making great advancements that enable many security improvements. EEI recognizes that the existing CIP reliability standards may be overly prescriptive and at times drive unnecessary costs, while limiting security benefits available through the application of modern technology. Nevertheless, fixing these problems needs to be taken a step at a time to avoid disruption to existing systems and processes used by companies. EEI encourages the SDT to focus more on how virtualization might be effectively integrated into BES Cyber Systems, under the current standards, rather than trying to solve all these issues at an early stage of industry adoption.

Given the pace of change of the CIP reliability standards to which the industry has been responsive and will continue to be responsive as it contemplates upcoming compliance effective dates, the members who participated in the development of these comments do not, at this time, support the overly broad and sweeping changes proposed by the SDT. For these members, the modifications are premature and, while there are aspects of what the SDT is considering that may have future benefit and utility, employing those changes at this time could prove to be too disruptive to existing efforts by the industry. Furthermore, the use of virtualized networks within the industry is still limited and efforts to try and tailor the current body of standards to accommodate this emerging security solution is likely to create new security concerns. Instead, we encourage the SDT to work toward addressing the more immediate needs of the industry such as clarifying how the security and management of BES Cyber Systems can be accomplished in a virtualized environment using the existing body of standards, as currently approved. Additionally, EEI further suggests that the level of change being considered by the SDT may be better addressed through a separate initiative spanning several years to allow more engagement by the industry.

EEI also notes that, while the SDT has offered up some very interesting ideas to address virtualization within BES Cyber Systems, many Responsible Entities still feel there is a lack of overall clarity necessary to address the design, control, and protection of these systems in a virtualized environment.

EEI’s last concern centers on the auditability of the proposed approach. While the security objective-based approach does provide a friendlier environment for virtualization, there is concern that, from an audit perspective, this approach may prove to be difficult for Responsible Entities and auditors to demonstrate compliance leading to interpretations and judgements that could impact the security of BES Cyber Systems, while placing into question whether the proposed solution can be effectively and consistently audited.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1,3

Answer	
Document Name	

Comment

Hydro One supports the comments submitted by NPCC TFIST. In addition, the real fork maybe it is time to determine whether the CIP set of Standards are ready to be transitioned into a full risk-based set of standards (starting from CIP-002) rather than control-based set of standards. The SDT is trying to have it both ways for the sake of backwards compatibility. In the current proposed revisions, certain security controls are maintained mainly for routable protocols and objective oriented requirements are being introduced to address virtualization. backwards compatibility is a desired outcome but it maybe time for SDT to consider the following:

- Is the industry mature enough for a full risk-based approach to cyber security?
- Have the auditors figured out how to audit CIP standards in a more risk-based/objective oriented world?

Until the answer to both questions above are "yes", Hydro One recommends that the SDT develop one or more standard(s) with a set of controls applicable to virtualized components.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

LIZ – in conjunction with hardware separation makes sense, but by itself leaves a lot of opportunity for failure due to misconfiguration

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	
Document Name	

Comment

Regarding the definitions, please clarify how a virtual switch that is creating a LIZ should be categorized?

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer

Document Name

Comment

Santee Cooper appreciates the SDTs effort in drafting the complex virtualization standards.

CIP-005 1.1-1.1.1. Are you talking about a firewall or something else to logically isolate our systems? How could this be accomplished when using dial up? Will dial-up require the use of an EAMS?

CIP-005 2.1 - With the revised definition of Intermediate System and Interactive Remote Access does this mean an Intermediate System is required to connect with medium impact sites that use dial up? CIP-005 2.2 – With the removal of “with External Routable Connectivity” under applicable systems, are dial up connections going to be required to be encrypted?

CIP-005 2.3 – With the removal of “with External Routable Connectivity” under applicable systems, will multi-factor authentication be required for dial up systems?

CIP-010 – This is a situation where in the past the prescriptive model would be a better fit than the higher level objective based model. Currently this standard is specific on what the expectations are and what needs to be done to meet the requirements of the standard. In the proposed revision requirements they are too vague and leave it open to an auditor’s interpretation.

For entities not pursuing virtualization, these revisions tend to create more confusion around what is required for compliance.

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NYPA

Answer

Document Name

Comment

Moving to a security objective approach implies for a need for a cyber-security plan which considers the risk and appropriate mitigation and controls to meet the objective.

Likes 0

Dislikes 0

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP Member Group	
Answer	
Document Name	
Comment	

1. As written, the proposed changes in the standard package may add unintended compliance risk to applicable entities. The standard proposes flexibility to allow the responsible entity to implement controls for the Secure Configuration; however, this may not comport to audit situations where the auditors are deciding whether the entity's controls meets the auditors' expectations of compliance. The SSRG suggests anticipates the Implementation Guidance document to be posted in the future may relieve some of these concerns.

2. Questions to consider: How will the retirement of the defined term for EACMS affect the Order 848 FERC directed CIP-008 changes? Will CIP-008 need revising once this current project is approved by FERC? Should changes to CIP-008 be part of this exercise?

Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	

Generally speaking, Southern Company is in favor of this change in methodology. These changes will facilitate the use of more current and potentially more secure technology while allowing Registered Entities the flexibility to use virtualized or physical systems to do so. We recognize the inherent risk in any change to the compliance methodology and wish to embark on such changes taking care to balance the risk associated with the change with the benefits received from the change.

That said, additional clarity and technical guidance is needed in documenting a Secure Configuration. Southern would like to see more clarity in how far the Secure Configuration boundary goes. At this time, it appears overly broad and we are concerned that it may start to include things like firewall rules, iDRACs and other more in-depth configuration items.

Likes 0	
Dislikes 0	
Response	

Sean Cavote - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer

Document Name

Comment

PSEG supports the comments made by EEI and the Long Island Power Authority.

Likes 0

Dislikes 0

Response

Jack Cashin - American Public Power Association - 4

Answer

Document Name

Comment

APPA recognizes the complex and difficult job the SDT had in drafting the virtualization standards. The SDT’s efforts are appreciated. Project 2016-02 provides best practices for security standards that strive to stay ahead of adversaries’ efforts. The Project is groundbreaking and is the first step toward the next level of the best practices in security standards. APPA acknowledges that the comments herein largely question the draft standards and request clarity. Because the questions are open ended, public power did not see a need to provide yes/no answers, believing that is best left too registered entities. Public power sees this effort to date as significant progress.

Importantly, implementing the virtualization standards will be a challenge for NERC and industry. APPA, therefore, believes that the implementation plan and its timing is now the most crucial consideration. APPA encourages the SDT to draft an implementation plan with a two- to four-year implementation phase. The implementation plan needs to be facilitated by sufficient guidance. Guidance will need to be provided during implementation based on best practices learned during the implementation period. The period of putting Project 2016-02 in place should be a phase of learning so that best security practices can be implemented by all entities big and small. Because these changes are extensive, involve complex new concepts, and may have many unintended consequences, a pilot project involving volunteer utilities and NERC should be part of the implementation effort for these changes, similar to the pilot performed for the CIP v5 transition.

To reiterate, the following are some general principles that might be applied to guide revisions to the proposed virtualization changes:

1. APPA supports the SDTs efforts on proposed changes and believe this is a great initial step.

2. Changes are more extensive than expected, probably have many unintended consequences, are complex and largely untried, and in some cases expand CIP scope to address new vulnerabilities introduced by virtualization.

3. Therefore, consider a parallel “virtualization overlay” approach, in which the existing definitions and requirements are retained, but the proposed new definitions and new requirements are also an option. An entity must identify which approach they choose, on a cyber-system by cyber-system basis.

4. The overlay approach might sunset after a time or be reassessed at a certain point based on lessons learned.

5. Expansion of CIP scope to address new vulnerabilities associated with virtualization should be restricted only to virtualized BCS. These changes should not increase scope for non-virtualized BCS. 6. Public power strongly urges that a NERC-sponsored pilot project with volunteer utilities, as happened with CIP v5 changes, be utilized with virtualization.	
Likes 0	
Dislikes 0	
Response	

Virtualization Informal Posting Consideration of Comments

Project 2016-02 Modifications to CIP Standards

The standard drafting team (SDT) for Project 2016-02 Modifications to the CIP Standards, investigated the issues and unique risks associated with virtualization technologies. During the SDT's review, it was discovered that accommodating virtualization technologies in the CIP standards could affect many of the technical definitions, such as the foundational "Cyber Asset" used within CIP standards, and also the technical CIP standards (CIP-005, CIP-007, and CIP-010). Virtualization changes fundamental assumptions and some legacy standards requirements. There is no longer a need to prescribe the Electronic Security Perimeter (ESP) and Electronic Access Point (EAP) architecture with perimeter-based security or the exclusive use of routable protocol. The SDT found virtualization to be not only a driver of change, but also a pointer to a larger issue with the standards' adaptability to current and future technology innovation.

The SDT concluded that the more technical standards could benefit from removing inherent prescription of certain architectures and topologies, and moving requirements to an objective or results-oriented level that do not make assumptions about architecture. In other words, the SDT asserts that the standards should not prescribe how to secure today's newer architectures. Rather they should require that certain security objectives be met regardless of topology or architecture. In doing this, the standards will support virtualization and other future innovations that can increase reliability, resiliency, and security of our BES Cyber Systems.

The SDT posted the virtualization work that was completed to date for an informal posting November 2 to December 18, 2018. There were 76 sets of responses, including comments from approximately 199 different people from approximately 132 companies representing 10 of the Industry Segments.

The SDT thanks the industry for the time and attention given to these matters and the resulting comments. The SDT captured some of the overall themes from all the comments received to focus the SDT's efforts as we progress towards a formal posting.

Overall Themes

- Several commenters questioned the need for changes to requirements since virtualization is not prohibited and several entities have undergone successful audits on virtualized systems. An example of one of the fundamental issues would be when a Cyber Asset or an entire BES Cyber System and its associated systems (not only hosts, but storage, networks, EAPs, etc.) become logical constructs composed of software and data only. In response, the SDT will focus on communicating the case for change; why some changes are needed to allow different architectures and approaches that can significantly improve cyber security in virtualized environments but do not fit well with standards such as CIP-005. Virtualization technologies also present some unique risks that should be addressed.

- Commenters had suggestions on approaches they believe would help alleviate the amount of change to the current standards. The SDT will consider each approach as the team moves forward determining what changes can and should be made to the standards.
- Commenters pointed out some issues with the move away from the Cyber Asset level to a system level approach. They raised the concern this could cause an industry wide CIP-002 reassessment of all systems. They also pointed out that the systems concept has been used to group devices of like attributes (such as Operating Systems) for ease of reporting evidence on a per requirement basis. This type of grouping interferes with the concept of “Each BES Cyber System must be in a logical isolation zone.” The SDT is considering how to incorporate changes based on these comments.
- Several commenters spoke to the security objective statements within the requirements. While there was support that objectives do provide clarity about the goal of a requirement, commenters suggested they are written too broadly, which introduces auditability concerns. The SDT will work towards drafting objective and measurable requirements.
- Almost all commenters responded to the removal of the term “programmable” within the definitions as we were looking at a full move to a systems approach. The concern was over the potential to bring in non-cyber components of systems such as electro-mechanical devices. The SDT will work on restoring the programmable terminology.
- Commenters suggested the Logical Isolation Zone (LIZ) concept needs further refinement and explanation. The SDT is considering refining this concept or identifying other options to clarify how security requirements will be applied within the standards.
- Commenters generally agreed with splitting out the ‘monitoring only’ portion of Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) and treating that security risk at the information level. Some commenters suggested that the applicability of Electronic Access Monitoring Systems/Physical Access Monitoring Systems proposed in CIP-004 needs further review because it would continue to prevent the use of monitoring services. The SDT is continuing to consider options to allow monitoring information to be treated as BES Cyber Security Information to limit the scope of applicability.
- The proposed CIP Exceptional Circumstances (CEC) additions met with approval though several commenters suggested that all CEC phrasing should be at main requirement level. The SDT has considered this but must balance whether or not a CEC should be available for every requirement part. In those cases where the CEC does apply to every part it was moved to the main requirement.
- Many commenters suggested the Secure Configuration concept involved a fairly broad scope expansion from five discrete software items to numerous areas that would also include methods and processes. They believe that these would be difficult to inventory because they are not necessarily discrete items. Commenters suggested that several of the items in a Secure Configuration as defined are procedural, which conflicts with the change management requirement. Some pointed out that methods could differ per system, times thousands of systems. The SDT will continue to consider options to address the objective level requirement changes to limit the scope of change.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Unofficial Nomination Form

Project Number 2016-02 Modifications to CIP Standards

Do not use this form for submitting nominations. Use the electronic form to submit nominations by **8 p.m. Eastern, Friday, March 29, 2019.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information can be found on the Project 2016-02 Modifications to the CIP Standards page. If you have questions, contact Jordan Mallory (via email), or at 404-446-2589.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Project 2016-02 Modifications to CIP Standards

This solicitation for nominations is to augment the existing Project 2016-02 Modifications to CIP Standards drafting team that is continuing to address the Standard Authorization Request. NERC is seeking individuals from the United States and Canada who possess experience in one or more of the following areas, but are not limited to:

- Virtualization;
- Cooperative representation;
- Canadian representation; and
- Guidelines and Technical Basis representation.

Standards Affected

CIP-002-6, CIP-003-7, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, CIP-011-2, and CIP-012-1.

The time commitment for this project is expected to be up to four face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Name:	
Organization:	
Address:	
Telephone:	
E-mail:	

Please briefly describe your experience and qualifications to serve on the requested Standard Drafting Team (Bio):

If you are currently a member of any NERC drafting team(s), please list each one here:

☐ Not currently on any active SAR or standard drafting team.

☐ Currently a member of the following SAR or standard drafting team(s):

If you previously worked on any NERC drafting team(s), please identify each one here:

☐ No prior NERC SAR or standard drafting team.

☐ Prior experience on the following team(s):

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:

☐ Texas RE	☐ NPCC	☐ WECC
☐ FRCC	☐ RF	☐ NA – Not Applicable
☐ MRO	☐ SERC	

Select each Industry Segment that you represent:	
☐	1 — Transmission Owners
☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators
☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:	
☐ Balancing Authority ☐ Compliance Enforcement Authority ☐ Distribution Provider ☐ Generator Operator ☐ Generator Owner ☐ Interchange Authority ☐ Load-serving Entity ☐ Market Operator ☐ Planning Coordinator	☐ Transmission Operator ☐ Transmission Owner ☐ Transmission Planner ☐ Transmission Service Provider ☐ Purchasing-selling Entity ☐ Reliability Coordinator ☐ Reliability Assurer ☐ Resource Planner

---

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

Provide the names and contact information of two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		E-mail:	
Name:		Telephone:	
Organization:		E-mail:	
Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Nomination Period Open through March 29, 2019

Now Available

Nominations are being sought for standard drafting team members through **8 p.m. Eastern, Friday, March 29, 2019**.

Use the electronic form to submit a nomination. If you experience difficulties using the electronic form, contact Wendy Muller. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies and the project page.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Project 2016-02 Modifications to CIP Standards

This solicitation for nominations is to augment the existing Project 2016-02 Modifications to CIP Standards drafting team that is continuing to address the Standard Authorization Request. NERC is seeking individuals from the United States and Canada who possess experience in one or more of the following areas, but are not limited to:

- Virtualization;
- Cooperative representation;
- Canadian representation; and
- Guidelines and Technical Basis representation.

Standards Affected

CIP-002-6, CIP-003-7, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, CIP-011-2, and CIP-012-1.

The time commitment for this project is expected to be up to four face-to-face meetings per quarter (on average two full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome.

Next Steps

The Standards Committee is expected to appoint members to the team in April 2019. Nominees will be notified shortly after they have been appointed**.**

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Virtualization and Future Technologies

Project 2016-02 Standards Drafting Team: The Case for Change

April 2019

Table of Contents

Executive Summary

What the interconnected power grid does for Bulk Electric System (BES) reliability, virtualization does for the computing infrastructure supporting vital control systems. Individual utilities interconnected their power systems to form a power grid to share spare capacity for meeting demand peaks and surviving contingencies such as generating unit and transmission line outages. Virtualization connects processors, networks, and storage into ‘computing grids’ that allow our vital systems and applications to meet peak demands and survive outages of individual components.

This is accomplished by abstracting servers, networks, and storage into virtual or logical resources that can be independent of specific underlying hardware such as individual processors, circuits, and disks. A control system and its underlying operating system become a virtual machine and can move to any available hardware. This greatly increases reliability and resiliency of our control systems that support BES reliability.

Virtualization technologies also allow enhanced cyber security controls and the ability to move access controls from the edge of our networks to much deeper inside of them. This is analogous to having generation close to load centers to reduce the susceptibility to outages. These newer security controls allow us to provide tighter security by moving access controls from an outer perimeter closer to the actual code performing reliability tasks.

Virtualization and advanced technology are challenging the way we characterize the Critical Infrastructure Protection (CIP) standards’ objectives and how we develop technical requirements. Use of virtualization and advanced technology can provide benefits for implementing both operational and security enhancements to a system. The goal is to require technology-enforced controls as alternatives to the current prescriptive requirements like those requiring a physically structured architecture, without forcing the use of the new technology. The existing standards with their prescriptive language limit the ability to take full advantage of the new technologies. The Project 2016-02 Modifications to CIP Standards Standard Drafting Team (SDT) is drafting new requirements to support virtualization capabilities. This leaves Responsible Entities with the option to maintain a non-virtualized environment and use backward compatibility to preserve current CIP investments and security postures.

This white paper represents the views of the SDT and presents a sampling of virtualization concepts. It explains, in the SDT’s opinion, how the use of these concepts is inhibited by some of the CIP standards’ definitions and requirements. It also introduces the SDT’s ideas on how to address these issues while maintaining compatibility with current state. The goal is to allow for the use of these technologies and newer security controls by removing prescribed “how’s” and replacing them with clear “what’s” that would allow both current state and these enhanced features.

Introduction

Note: The Project 2016-02 SDT developed this white paper to explain the need to change the cyber security CIP Reliability Standards. This white paper has not been approved or endorsed by NERC and is solely the views of the Project 2016-02 SDT.

In the history of the CIP standards, industry has seen many versions and changes. Some have been straightforward and almost self-explanatory. Others, complex and time-consuming to implement. Still others have been foundational, like the ‘do-over’ change from Versions 1 – 3 to Version 5. Not surprisingly, the prospect of another set of fairly major changes, this time involving virtualization sparks a great deal of industry concern. It raises valid questions about the timing and the drivers of those changes, and whether or not they are truly necessary. The white paper is designed to provide detailed answers to those questions from the viewpoint of the SDT. This introductory section provides a short, high level introduction to the white paper discussion on what brought about the SDT’s focus on future revisions to the CIP standards to address virtualization.

Recognizing the continuing growth in technology innovation, many entities in the Electricity Sector have implemented virtualization as part of their CIP programs. Many of these same entities, however, have implemented this new technology without taking full advantage of virtualization’s advanced capabilities. There are a number of reasons for this from the constraints of the current CIP architecture to the ongoing ambiguity around how new virtualization technology applies to CIP compliance. Some of those who are implementing virtualization are experiencing a great deal of uncertainty and difficulty around developing implementation strategies that will support compliance and achieve greater reliability and security.

These issues began coming to light following the NERC “Virtualization Summit” in 2015. Ultimately, the Version 5 Transition Advisory Group (V5TAG) heard about the industry concerns and determined that the issues around the standards and virtualization would be best addressed by a drafting team. The Project 2016-02 SDT was assigned the task to address the technological innovation in virtualization within the CIP standards.

The SDT’s purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards. The SDT’s intent is to better position the CIP standards to be applicable to any future technological innovation. Leveraging the abstraction that virtualization provides will allow the industry to more readily adopt new technology and increase security posture. This paper presents the SDT’s case for change to the NERC CIP standards that is needed to allow for the innovative security techniques and new concepts brought about by virtualization.

As virtualization has progressed, many of these types of issues cannot be addressed with Implementation Guidance. Documenting a possible way to implement a requirement is of great value, but Implementation Guidance cannot, for example, change current requirements so they do not prescribe a perimeter-based model, or allow remediation VLANs. It also cannot add new requirements that are needed for issues like management plane isolation or handling shared infrastructure. These new concepts and techniques require changes to the standards to make them viable and to clarify how they should be secured.

Chapter 1: Virtualization Benefits

The most basic concepts of CIP are essentially unchanged from the Urgent Action 1200 standard in 2003. The primary focus of those standards was the "critical cyber asset"; an "electronic device" such as a server, workstation, or relay as a physical object. It had an operating system, always on and performing its function, and communicating with other components over routable protocols. It was protected by traditional firewalls at the network edge looking at source and destination protocol addresses and ports as the only mechanism by which to make network access control decisions.

Figure 1

Today, virtualization has changed this scenario. With virtualization, physical devices are no longer the primary units of organization. An entire control system infrastructure can be virtualized (such as "software defined data centers") and only exist as logical constructs. An EMS database server may never exist as a discrete physical object. With containers (operating system emulation), there may not be a concrete tie between application logic and an operating system. Virtual machines can be created and destroyed dynamically and are neither always on, nor tied to specific hardware. Workloads may mirror their information for reliability purposes across great distances without using routable protocols. With micro-segmentation, network access control lists are now much more granular than IP addresses at a perimeter. They are enhanced by policy-based control templates enforcing access at a "user to workload" level throughout the system infrastructure. Electronic access control may no longer be based solely on routable protocol addresses or found only at an ESP boundary.

Benefits of Virtualization

Virtualization technologies bring many reliability benefits to BES Cyber Systems (BCS).

- Increased uptime, very fast recovery capability and flexible architecture that can instantly adapt to changing workloads.
- Virtualization allows for racks of CPUs, memory and disks to be tied together with high speed mesh networks and viewed simply as raw computing resources.
- If the workload on a particular virtual server is nearing capacity, the infrastructure orchestration system can create and configure an additional server on the fly, bring it online to help with the peak workload, and then destroy it when it is no longer needed.

- If a physical machine runs out of resources, the workload can be moved to another physical machine dynamically based upon relative load. When a virtual server or workstation is not in use, it is similar to a physical server that is powered off.
- This flexible and dynamic architecture also allows improved security controls such as those provided by micro-segmentation.
- Users can be granted access to specific workloads that can be placed dynamically throughout the infrastructure with managed access to provided services.

More secure, more reliable, cost effective technology solutions

New and innovative security capabilities continue to evolve to address current threats, particularly in virtualized environments. These capabilities can increase the security of hosted BES Cyber Systems. For example, *distributed firewalls* based on software defined access policies can enforce access controls at a much deeper level within the infrastructure to help prevent an attacker's lateral movement through the network. *Privileged introspection* allows security service such as anti-malware, to operate in a tamper-proof way outside of the instances they protect. *Zero trust models* allow communication to be protected end to end between individual processes across cyber assets without having to trust that devices in the path (such as all firewalls and switches) are configured correctly to protect the data. We'll consider each of these and other examples in more detail to show the benefits and the case for change in the CIP standards.

Chapter 2: Virtualization challenges in the NERC CIP Standards

Virtualization brings benefits to reliability and resiliency of our BES Cyber Systems. It also brings challenges with determining how some of the newer concepts fit within the framework of the NERC CIP standards. Some of these newer techniques and concepts are:

- Identification of Virtual Cyber Assets
- Distributed Firewalls vs. Perimeter models
- Zero Trust models
- Virtualized Firewall Interfaces
- Virtual Storage challenges
- Management Plane Isolation
- Privileged Introspection
- Remediation VLANs

Each of these topics will be covered in detail in the following sections.

Identification of Virtual Cyber Assets

One of the issues requiring change within the CIP standards is the need to clarify the treatment of virtual machines (VMs) under today's definitions. The foundational term Cyber Asset is defined as "Programmable electronic devices, including the hardware, software, and data in those devices." This definition, since it includes the hardware, does not fit with virtualized environments. A literal use of this foundational definition would mean a server hardware platform may be a BES Cyber System, the hypervisor software could be the "operating system", and all the virtual machines running on the hardware are applications or simply data. The CIP-007 requirements, most of which are aimed at an operating system instance, would not be applied to these virtual machines since they aren't hardware. This is referred to in the Figure 2 as the "Physical System w/Software Model."

To require that VM operating systems be classified correctly, the tie between a virtual machine and the hardware needs to be clarified. The standards and their associated definitions need to clearly support the "VM as a CA Model" (Virtual Machine as a Cyber Asset) as pictured in Figure 2. Here it is clear that the physical server hardware and the hypervisor are in scope and each VM is subject to requirements such as CIP-007.

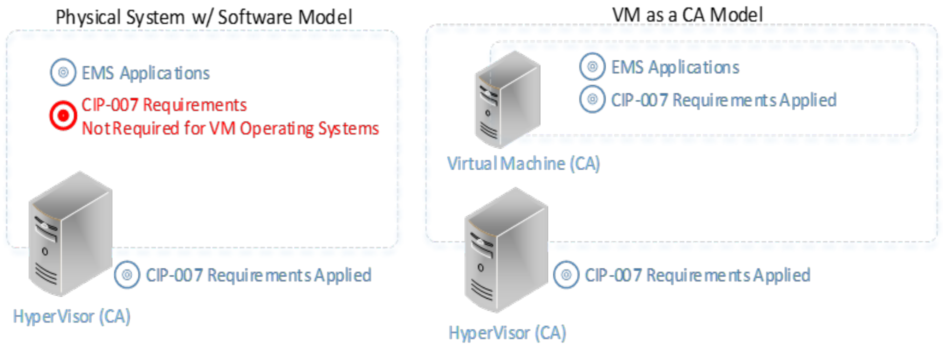


Figure 2

The Cyber Asset definition assumes a 1:1 relationship between a BES Cyber Asset and its hardware. Virtualization, however, breaks that concept because in some cases hundreds of virtual BES Cyber Assets can share a pool of hardware resources (compute, network, and storage). The outdated concepts need to be changed to recognize the one-to-many relationships that are now possible between a BES Cyber Asset, an instance of an operating system supporting applications, and the underlying hardware so it is clear how each is to be treated. There are three different types of asset classes involved in today's BES Cyber Systems:

- Self-contained devices that are composed of dedicated hardware, some form of operating system or firmware, and the application code. This is the traditional definition of a Cyber Asset and applies to things such as digital relays, RTUs, physical operator workstations and dedicated physical servers.
- Virtual "cyber assets" composed of an operating system and applications or containers minus any dedicated hardware. These types of assets are logical or virtual constructs by nature and exist only in memory or files. They can, however, appear from a network perspective the same as any other host.
- Shared Infrastructure consists of the hardware resource pools (compute, network, storage) and is shared by virtual cyber assets and can host numerous virtual cyber assets, networks, or storage locations.

The current CIP standards only recognize the first class and changes are needed to properly address the other two. This will allow BES Cyber Systems, which can be composed of all three asset classes, to be properly identified and classified and the proper requirements applied to each one.

Distributed Firewalls vs. Perimeter Models

Distributed firewalls based on software defined access policies can enforce access controls deeply within the infrastructure to help prevent an attacker's lateral movement through the network. The CIP standards (CIP-005) today require a perimeter-based model as shown in the left side of Figure 3. It has an Electronic Security Perimeter (ESP) as a logical border around a group of cyber assets, and defined interfaces (on a firewall for example) as an Electronic Access Point (EAP). This perimeter model is a prescriptive topology, and for many scenarios is still a valid way to perform network security. What may be prescribed, however, for a small network of similar cyber assets may not be ideal for a large network of virtualized BES Cyber Assets.

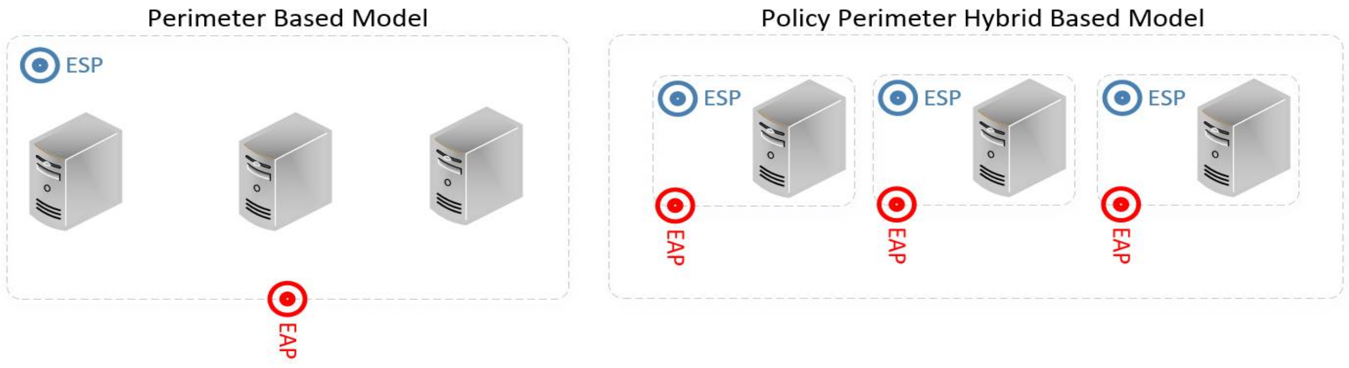


Figure 3

The issue is that network access is permitted or denied at the outer EAP "gate." Even if access is only needed to a single cyber asset inside the perimeter and a strict rule is instituted at the EAP "gate" to allow someone access to that single cyber asset, that control is implemented only at the gate. Once inside the perimeter, there are no network level access controls that would prevent hopping ("pivoting") from that cyber asset to all other cyber assets inside the perimeter. Attackers today depend upon this; if they can get a foothold on a single cyber asset inside a perimeter they can work over time to move laterally within the environment from there.

Virtualized environments, especially those of cloud providers that support tenants from various customers, had to be designed to implement new, more granular security techniques to not only mitigate this threat but to also keep customer's workloads totally isolated from one another. These new techniques are philosophically simple – every cyber asset is inside its own "perimeter" and the EAP "gates" are specific to each virtual cyber asset. This is shown on the right side of Figure 3 in the "Policy Perimeter Hybrid Based Model." In this model, network access is controlled at an individual cyber asset level and access to a single cyber asset gives you no additional access to any other cyber asset. An attacker's ability to move laterally or pivot in this environment is greatly reduced. These techniques are also configured at a *network access policy* level and the infrastructure dynamically implements it at various levels throughout the entire infrastructure. Even as these cyber assets move dynamically within the infrastructure, these access controls move with them. All of this, however, precludes the ability of administrators to provide a "list" of potentially hundreds or thousands of ESPs, EAPs, or the discrete rules per EAP. This is because it is all dynamically generated by the infrastructure to control access in accordance with a higher-level access policy.

These same techniques can be used to mitigate the same risks within virtualized CIP environments. The problem is that CIP requires the perimeter model with EAP "gates" as the only prescribed way to implement network level security. The SDT is planning to change the CIP standards and definitions in a way that does not *preclude* the perimeter based model, but also does not t *prescribe* that model as the only way. For example, the language in CIP-005 R1.2 "All External Routable Connectivity must be through an identified Electronic Access Point (EAP)." This creates an issue since historically this is a physical interface on a physical device. More current, virtualized architectures distribute the policy enforcement tasks to multiple devices and each of them validates that the network communications passing through it are permitted. The current standards do not align with these architectures because there is no single interface identified that is responsible for policy enforcement.

Identifying non-routable EAPs and the OSI Model

Related to the ESP issue, today's CIP Standards are limited to prescriptive topologies even as potentially more secure, reliable and cost-effective solutions are available. ESP's are defined today by the access provided at the network layer (OSI Layer 3) and are therefore limited to making access decisions based on routable protocol addresses. This method does not support security evaluation or compliance via security solutions at any of the other layers of the OSI model. This presents two issues:

- There may be network access into and out of the perimeter at different layers other than by a purely routable protocol that allow for things like high speed replication of data. This will be discussed further in the "Multi-Site Data Center Extensions (Super ESP)" section below.
- Virtualized environments have much more context and can enforce network access control at more granular levels in much better ways. These include by user, process, or certificate and are not limited to only a source/destination IP address of a routable protocol.

In many environments today, the perimeter model is sufficient and routable protocol addresses are all an entity has to make access control decisions. However, the standards should not prescribe this as the only way and should allow entities to use these more granular controls that may operate at other layers.

Zero Trust Models

The zero trust network model is a new and different way of thinking about network security. In most cases it can be implemented within the security model that an entity currently has deployed.

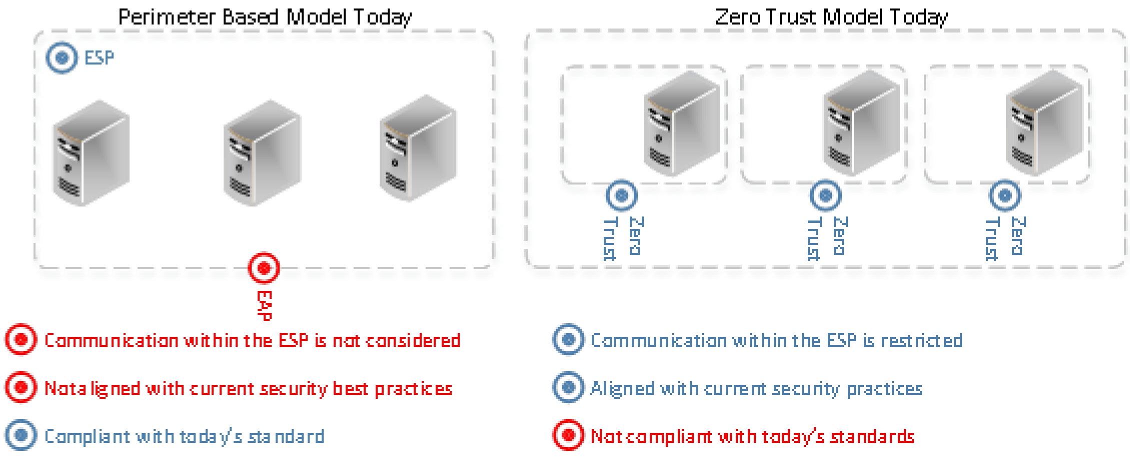


Figure 4

Most entities have a perimeter model deployed, which is what the current ESP model requires as in Figure 4. Traditionally, this consists of a firewall (or firewalls), with a single path into the network (EAP). This model protects the BES Cyber System indirectly, by protecting the network topology. This access point is protected by rules and policies that tell the firewall what kind of traffic to pass and what kind of traffic to stop. This model can be loosely compared to a gated community, where the fence is the firewall, and the gate and security guard are the access control.

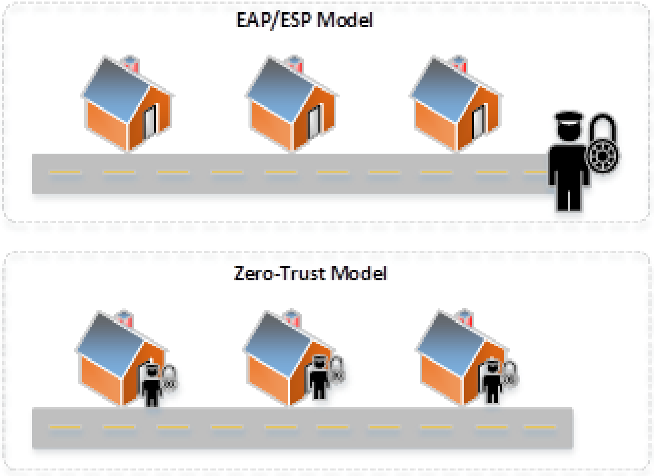


Figure 5

The overarching problem with this model is that if attackers should get past the firewalls and through the gate, they would have free rein throughout the network and could pose a serious threat to other BES Cyber Systems within the ESP.

A zero trust model brings the protection directly to the cyber asset or even to the process level. Using network policies, whitelisting, certificates, and other technologies, the ability of an intruder to move around is severely restricted. A zero trust model usually starts with simple items like restricting network traffic to the device except that which is necessary for it to perform its job function. It also restricts what logins can access the device. Finally, it introduces more complex ideas such as digitally signed executables, restrictions on what time a process can be started, and end to end encrypted traffic, even within the local network. This model protects the BES Cyber System directly by protecting the workloads, the devices and the topology. Unfortunately, this model is very difficult to describe using the current language constructs of the CIP requirements.

Referring to the gated community analogy in Figure 5, this would put a fence in every yard, a lock on every door and an alarm system in every house. This effectively isolates the intruder to the public areas of the neighborhood.

Virtualized Firewall Interfaces (‘Firewall on a Stick’)

As the use of network segmentation grows and firewalls are used to control traffic flows between the network segments, firewalls need higher densities of interfaces. To obtain these higher densities, products today rely on fewer physical ports and instead use virtualized network interfaces to emulate many physical interfaces. Some modern firewalls are service modules (a “firewall on a stick”) installed in a switch or router where virtual interfaces are the only option to route traffic to and from the firewall as shown in Figure 6.

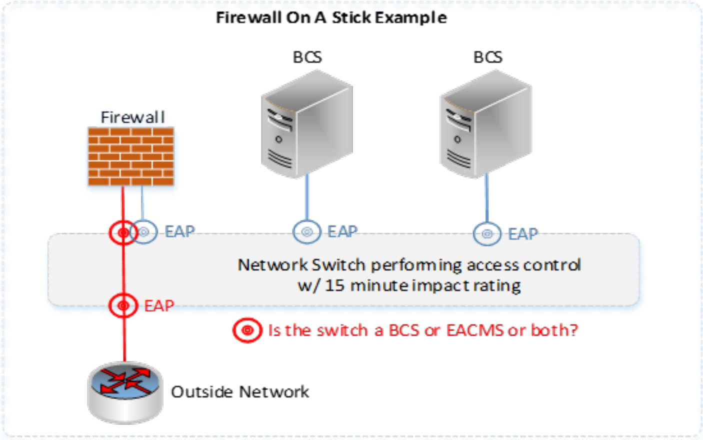


Figure 6

The CIP standards are ambiguous on how to properly identify these assets. If this were simply a network switch allowing two BES Cyber Systems to communicate with each other with a 15 minute impact if the switch is unavailable, then the switch itself is part of a BES Cyber System. In this example, the entity wanted to increase security of the communications between these two systems. To accomplish this, it put each BCS on its own network segment so it can filter all traffic between these two systems through a firewall. A “firewall on a stick” is installed in the switch and the ports on the switch are divided into virtual networks so the traffic between different segments is directed to the firewall and controlled. Since the firewall either has no physical interface or may use its few physical interfaces for redundancy, the outside network must connect to the same switch and that port is configured to the “outside” interface of the firewall. All communications to and from the outside network and between the two BCS are all controlled via the firewall. The entity has increased the security of these systems, but it is now undecided on how to identify the cyber assets in this scenario. As one example, are all the network switch ports now EAPs on an EACMS, or is this switch still just a part of the BCS? As access control is pushed deeper into networks as in this example, the current paradigms are ambiguous. The answer may lie in identifying new asset classes and developing new objective requirements that do not include prescriptive network topology assumptions. Trunks and sub-interfaces are common network technologies to aggregate data streams and better utilize limited physical interfaces[1].

---

[1] Trunking is the use of a single link to aggregate multiple data streams. This technology is widely used in networking and telecommunications. Sub-interfaces allow for multiple LAN segments to share a common physical interface.

Virtual Storage Challenges

As we move to virtual storage, there are issues with some of today's CIP concepts. For example, the CIP-011-2, requirement R2 restricts unauthorized access to BES Cyber System Information on systems meant for reuse outside of the CIP environment or systems meant for disposal. This causes a challenge for virtualized infrastructure. Today, when disposing of a physical medium or high impact BES Cyber Asset, access to BCSI can be restricted by sanitizing or destroying the media associated with the physical asset. If storage media is provided from a Storage Area Network (SAN) or Network Attached Storage (NAS) array, there may be no easy way to identify the specific drives where the data might have been stored. Additionally, there is no significant benefit to pulling drives from an array to sanitize or destroy them if there is another way to manage this media.

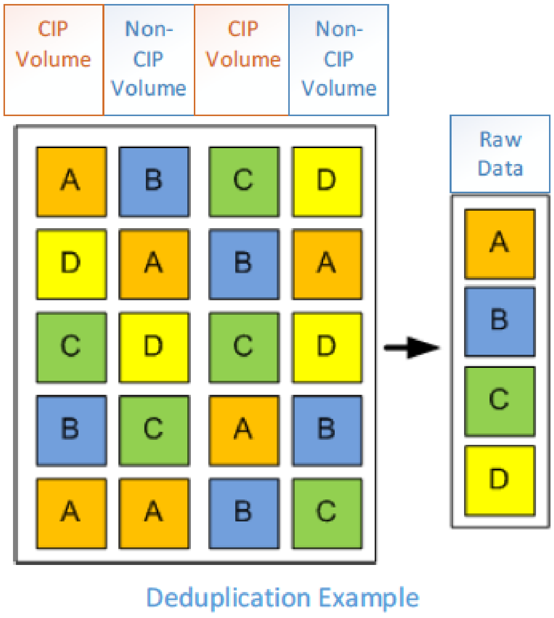


Figure 7

To extend this challenge further, many SAN and NAS environments can de-duplicate and move data to various storage tiers within the array to optimize access times and reduce latency. This process analyzes the data in small enough chunks to create single instances of data that are used within multiple volumes that may be assigned to any number of devices. The chunks with the highest access rates are then placed on fast storage media because the data is constantly referenced. This effectively causes data re-use if storage media is shared between CIP and Non-CIP assets even when the information contained within these de-duplicated chunks is not readily retrievable individually.

That was one example. The CIP standards were built on a paradigm of disk storage being physical disks dedicated to a Cyber Asset. Updates to the standards are needed to reflect the realities of virtual storage technologies that are in use today.

Management Plane Isolation

Because virtualized servers, networks, switches, firewalls, and storage are logical constructs, controlling access and communications to the management plane of these systems is imperative. Access to the management plane (interface/console/etc.) allows a user to create, modify, or delete these objects or entire infrastructures from one place, or move objects from one zone or network to another. Administrative level or "management plane" access to the hypervisors is therefore absolutely critical to the security and reliability of the hosted systems. These types of access must be brought into the scope of CIP standards if hosting BES Cyber Systems and will require changes to the CIP standards.

Another challenge of the perimeter model is it can drive less secure topologies in order to provide clear adherence to the perimeter model. In Figure 8 below on the right is the desired separation between the management plane of a virtualized environment and the production or "data plane". The management port of the BCA is connected to a switch on the management network. The production network switch is connected to the network interface on the BCA. This creates two different network paths to the BCA: one for normal production traffic and a separate network path with separate access controls for administrative or management plane access. It is unclear, however, if the BCA has now created two ESP's with two EAPs, and whether or not it is now an EACMS. It is not functioning as an EACMS, but from the topology it appears as one. The prescriptive CIP model may create a temptation to place the management interface into the production ESP as in the picture on the left. This is very clear from a CIP standard adherence perspective but is the less secure choice.

Figure 8

Privileged Introspection

Privileged introspection allows security services, such as malware detection, to be performed outside of the operating system and applications it is protecting in a tamper-proof way. Previously, malware that could gain elevated privileges on a cyber asset could then disable security services such as anti-virus solutions running on the same OS. Virtualized environments, however, can allow privileged introspection where anti-virus or application whitelisting services run as part of the hypervisor; outside of the operating system they are protecting so malware with elevated privileges inside the OS cannot reach them. Another benefit of privileged introspection is it allows integration with distributed firewalls because it can inspect network traffic entering or leaving virtual machines and make decisions with vastly more context. For example, these firewalls can control access not simply at a network address level (IP source/destination) but down to the level of a process with a particular certificate.

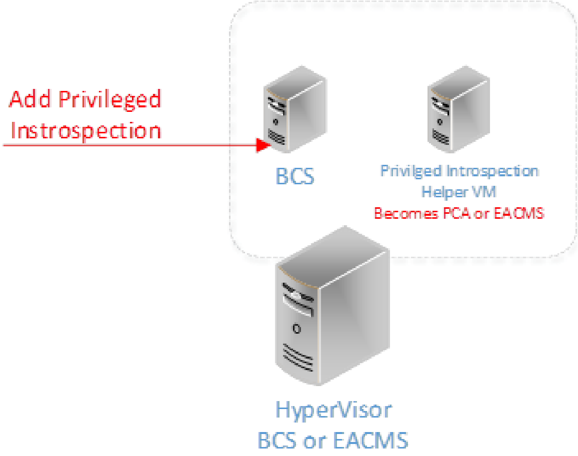


Figure 9

Even though the current CIP-007 R3 is already written at a security objective level and can work with privileged introspection, there can still be CIP standards issues brought into play. If this functionality uses "helper VMs", it is not clear how to identify and classify these under the current CIP standards. Since the status of malware detection is now outside the VM's, it requires grouping the VM's protected by privileged introspection into a particular BES Cyber System.

Remediation VLANs

As another example of the need for change in the CIP standards brought about by new virtualization technologies, CIP-010 R3.3 states, "Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset..." This is a valid requirement that cyber assets be in a CIP compliant state before being added to a production CIP environment. The issue is that this is written with the idea that an entity's new cyber asset is a separate physical asset it can configure in a compliant state prior to it being placed in a "production environment" and connected to a production network.

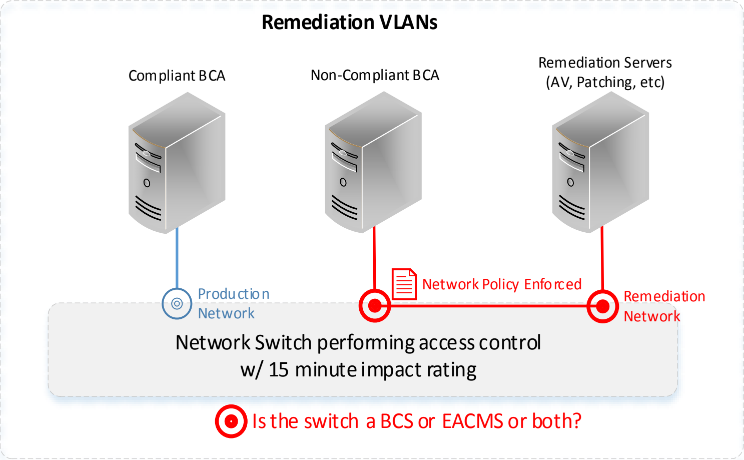


Figure 10

Virtualized environments, however, allow for a concept known as remediation VLANs. When a new cyber asset, such as a server or operator workstation is instantiated from an image, it is already "in" a production environment. However, it is brought up in a remediation VLAN where its network visibility is restricted to those services (patching, anti-virus updates, etc.) that it needs to assess vulnerabilities, update itself, and become compliant. Only after it is fully compliant with policy, can it be moved to a production VLAN where it has the full network visibility. Should this virtual machine become non-compliant with the network policy, it is moved back to the remediation VLAN to be made compliant again. This is an advanced security control, beyond what CIP-010 envisions, where real time checks are performed to ensure a cyber asset is compliant with security policy. The way the CIP standards are currently written, however, could preclude such advanced controls since this Remediation VLAN must be either part of an ESP or a separate ESP in order to host BCAs per CIP-005-5 R1. Requirements such as those in CIP-005 and CIP-010 need to be modified to allow for these more advanced features and controls.

Multi-Site Data Center Extensions (Super ESP)

There are technology solutions now that support very high levels of resiliency, so much so that virtual machines can be seamlessly moved from physical infrastructure at one data center across great distances to physical infrastructure at another data center. For example, control center functions could move easily and seamlessly from a primary control center to a backup control center across town or across the state. For this to work, an entity would use tunneling protocols that make the two data center networks appear as one local network ("layer 2 adjacency"). You've "stretched" a LAN across a WAN. The issue with CIP is that it assumes a LAN at each site with a defined ESP and access control at a point on that ESP at each site, with all the WAN communications equipment in between these ESPs exempted from scope. In

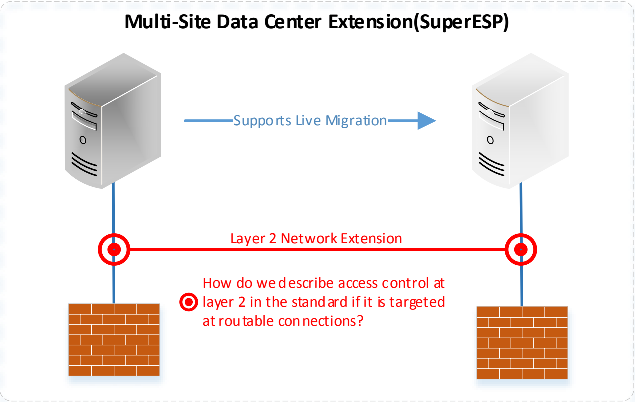


Figure 11

this situation, however, we have a single “local network” stretched between different sites creating at one level a “Super ESP”. Complicating the issue is that underneath this logical network extension, the data may actually ride in encrypted tunnels created at a routable protocol layer. At that layer, firewalls on an ESP can’t really provide any security, but that is prescriptively where the CIP standards say it must be done.

Chapter 3: Future Concept Example

Previously the proposed solution to address these issues with virtualization was a full embrace of the cyber system concept (retiring device level terms like Cyber Asset and BES Cyber Asset) and writing the technical requirements (e.g. CIP-005, CIP-007, CIP-010) at a more objective level. However, through industry feedback several important issues came to light:

- Eliminating the BES Cyber Asset definition and moving to the BES Cyber System as the sole foundational object with no further granularity would cause a complete overhaul and “do-over” of entities’ CIP-002 processes with insufficient benefit for the effort required.
- Requiring grouping systems by function exclusively conflicts with a number of different ways the industry has used the systems grouping flexibility; for example to group all Cyber Assets of a like operating system for patching purposes.
- Stating security objectives in requirements must be at a level where they are clearly measurable.

With these issues in mind, the future concept is to leave the foundational definitions largely unmodified. A “Cyber Asset” would remain as-is and be inclusive of the hardware as it is today. However, including the hardware for virtual cyber assets does not work, even though it needs to be protected the same as a discrete physical cyber asset. To resolve this the SDT will create a separate definition to capture virtual cyber assets so that they can be added to the applicability of the appropriate requirements. The hardware that provides compute, network, and storage resources would become its own new term to capture shared infrastructure and allow requirements to be written for risks unique to that environment. BES Cyber Systems would remain as-is and allow for all the various ways entities have used that concept to date.

The direction remains to establish objective level requirements but these need to be written at the appropriate level. For example, if CIP-005 R1 were written as “Mitigate the risk of unauthorized network access”, it is certainly an objective but is too high level to be measurable. No one would be able to state when, or to what degree this objective had been accomplished. If CIP-005 R1 were written as “Only allow known valid layer 3 IP addresses into or out of the network and implement this only at a Cyber Asset interface located only at the network edge”, it would be a prescribed topology and a prescriptive “how.” This should be avoided as it precludes much of the newer technologies presented in this paper. The latter is essentially the CIP-005 R1 of today and is one of the primary requirements that needs to change to remove this prescriptive topology and “how’s”.

An example of an alternative objective requirement that clearly describes a measurable “what” but avoids prescriptive “how’s” for CIP-005 R1 could conceptually be:

> *Deny all access to and from the networks on which high and medium impact BES Cyber Systems and their associated PCAs are connected and only allow network communication that has documented access permissions including the reason for granting access.*

This is a much clearer objective to accomplish but it avoids telling the entity how or where they must implement it or how their network must be architected. As for backward compatibility, an entity could still define an ESP with designated EAPs and provide firewall configurations as they do today. However, an entity using the advanced virtualization techniques from earlier in this paper, or future techniques to control network access that have not yet been contemplated can still show they meet this same objective.

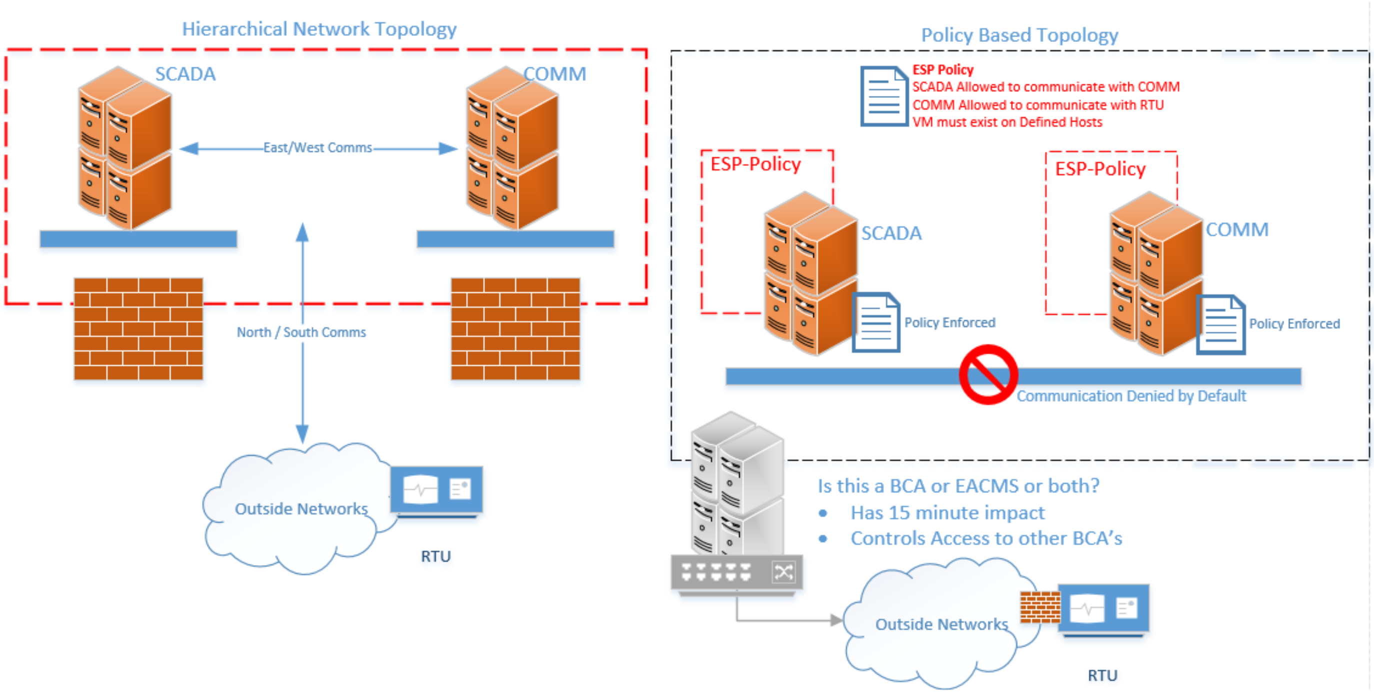


Figure 12

As shown in Figure 12, the current state ESP/EAP model on the left continues to be a valid architecture and topology with which to meet the objective. It is prescribed under the current requirements, but is not the ONLY way to accomplish the objective. On the right is a policy-based model in a fully virtualized system which can also accomplish the same objective once it is no longer prohibited by the requirement language. It has no distinct EAP; no distinct 'point' or 'interface' where the access controls are implemented. This is because the access policy is implemented throughout the infrastructure and the controls move with the virtual workloads. Access control is applied at a deeper level, closer to the functions that require protection and the policy allows no communication to occur that isn't explicitly allowed. The objective stated in the requirement can be met in either scenario.

For the asset classification, nothing changes for the architecture on the left. For the virtualized architecture on the right, the concept is to clarify that the systems in orange are virtual cyber assets, but without including the hardware. They exist as a virtual entity and need much of the same protection as a physical cyber asset. The systems depicted in grey are the Shared Infrastructure, a new asset class that hosts virtual cyber assets. Having these additional asset classes would allow the CIP standards to require protection appropriate to each class, whether a discrete physical system, a virtual cyber asset, or shared infrastructure hosting many virtual BES Cyber Systems.

]

Chapter 4: Conclusion

This paper has stepped through the benefits of virtualization in terms of increased reliability and resiliency for BES Cyber Systems. It also discusses how virtualization provides newer techniques for securing access to those systems, such as distributed firewalls and zero trust models. It has highlighted some of the issues created by several of these concepts and the required topologies contained within today's CIP requirements. Many of these issues revolve around the proper classification of cyber assets in virtualized environments and having asset classes whereby requirements can be properly scoped. Several other issues revolve around the prescriptive "how" of today's CIP-005 ESP/EAP model, the CIP-010 data requirements in a virtual storage world, or how CIP-011's requirements need minor changes to allow for technologies such as remediation VLAN's.

The CIP standards require some changes to:

- Address risks unique to virtualized environments such as the sharing of hardware resources and management plane access.
- Provide clarity around how to identify and categorize the various types of cyber assets in a virtualized infrastructure and scope requirements appropriately.
- Allow entities to fully implement newer security techniques in these environments that can provide higher levels of access control that are easier to manage, and don't require purchasing extra hardware to show compliance with prescribed topologies.

Many of these issues can be addressed as shown in the CIP-005 R1 example concept, where the prescriptive 'how' has been removed and replaced with a clearly stated security objective – one that fully allows for current state but also allows these newer techniques. Developing technology-agnostic security objectives can not only solve the issues presented by today's virtualization technologies, but also help address future issues brought about by technologies that aren't even contemplated today.

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Virtualization and Future Technologies: Case for Change White Paper

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on the **Virtualization and Future Technologies – Case for Change White Paper**. Comments must be submitted by **8 p.m. Eastern, Friday, June 28, 2019**.

Additional information is available on the project page. If you have questions, contact Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

Background Information

Many entities in the Electricity Sector have implemented virtualization as part of their CIP programs. Many of these same entities, however, have implemented this new technology without taking full advantage of virtualization's advanced capabilities. There are a number of reasons for this, from the constraints of the current NERC CIP standards architecture to the ongoing ambiguity around how new virtualization technology applies to CIP compliance. Some of those who are implementing virtualization are experiencing a great deal of uncertainty and difficulty around developing implementation strategies that will support compliance and achieve greater reliability and security. The Project 2016-02 Standard Drafting Team (SDT) was assigned the task to address the technological innovation in virtualization within the CIP standards.

This paper presents the SDT's case for change to the NERC CIP standards. It discusses what is needed to allow for the innovative security techniques and new concepts brought about by virtualization. It outlines several technical areas where either prescriptive network topology in the standards or ambiguity around how to handle new security capabilities create issues. The paper then describes a high level way forward using new definitions for the virtualized environment. It also changes some requirements to technical security objectives, stating what security objective to achieve, but allowing the entity to choose the technology to accomplish it.

The SDT is interested in any comments you may have on the white paper.

Questions

1. Do you agree with the case for change based on the virtualization issues discussed in the white paper? Please provide comments.

   ☐ Yes
   ☐ No

   Comments:

2. Do you agree with the proposed path forward as discussed in the white paper? Please provide comments.

   ☐ Yes
   ☐ No

   Comments:

Virtualization and Future Technologies: Case for Change Webinar Q & A

Project 2016-02 Modifications to CIP Standards

The Project 2016-02 Modifications to CIP Standards Drafting Team (SDT) held a Virtualization: Case for Change Webinar on April 24, 2019. The following items are questions and answers from the webinar. The SDT encourages industry to review this document prior to responding to the Case for Change Informal Comment period.

Q1. The White Paper states "Here it is clear the physical server hardware and the hypervisor are in scope and each VM is subject to requirements such as CIP-007" (page 3). Is it the SDT's position that this is true for hypervisors ONLY containing EACMS?

A1. No, the Cyber Asset definition is used for all asset classes including EACMS, BCA, PCA, etc. and it is inclusive of hardware. What the SDT is pointing out is that:

- If the Cyber Asset definition is inclusive of hardware and;
- If the entity classifies their VM as a Cyber Asset; then the hardware is included in that definition.

Q2. With the Zero Trust Model, now it looks like it would allow the co-located systems without a separate EAP (gated) around the ESP, and allow VM's to be an EAP/ESP individually and would not be requiring physical segmentation from NON-Compliance systems.

A2. Zero trust is a methodology for implementing access control and integrity. In principle the services on top in this model would not even trust their own underlying architecture. We will talk later in the presentation about the SDT's strategy for handling mixed-mode or mixed trust systems through the use of new requirements targeted at new definitions.

Q3. Since a Cyber System can be one CA, doesn't the model on the right just provide defense in depth, like physical security?

A3. An ESP within an ESP? The SDT does not believe the standard should prescribe a particular technology solution to these issues. In addition, within the standard the entity's network access control is only measured at the network edge. We believe the entity does not get credit for the defense in depth strategy, so it does not encourage them to use it.

Q4. As you discussed the BCSI issues, how will this team work with the separate SDT working on BCSI?

A4. Both CIP SDTs will keep open collaboration regarding BCSI through the development of each project.

Q5. The Case for change paper speaks to Distributed Firewalls as a more secure option in a virtualized involvement. Why can't this approach be effectively used in today's environment either behind an identified EAP or have the large ESP broken down into multiple ESPs?

A5. The SDT does not believe the standard should prescribe a particular technology solution to these issues. Within the standard the entity is only measured at the edge and we believe the entity does not get credit for the defense in depth strategy so it does not encourage them to use it.

Q6. To clarify: if a hypervisor hosts EACMS and non-EACMS, is the hypervisor an EACMS? Are the other non-EACMS VMs high watermarked? We've been told EACMS do not high watermark like BCAs.

A6. The SDT believes that how to handle the described scenario is unclear. This is the primary reason that it was presented in the challenges section of this presentation. EACMS relies on the CA definition and the CA definition includes hardware.

Q7. In regards to VLANs on a switch and port security. If I am using a trunk port connecting to a firewall, would this make the switch an EACMS? When any type of port security is used, i.e. mac security or 802.1x ... would this also make the switch an EACMS?

A7. The SDT believes that this is also an area that needs clarity. Through our analysis the switch itself performing the access control could fall into the EACMS category. However, if it has a 15 minute impact it may also fall into the classification of a BCA.

Q8. Why is the SDT working on still addressing hardware instead of addressing the Virtual environment risk (using the highest risk application principle)? SDT is not the first to draft virtual security, PCI council and NIST already have a risk based approach.

A8. The SDT believes that it is not simply addressing the hardware but that the existing definitions are limiting our ability to describe virtual environments. We have been looking to other frameworks as guides to effectively describe these new technologies while maximizing our ability to be backward compatible with existing programs.

Q9. BCSI explanation was very confusing. If SAN is part of the environment, why should not the storage area be the focus?

A9. The SDT is addressing the storage architecture as a core area of virtualization as you will see on many of our drawings. While changes may be needed, we are not directly addressing the handling of BCSI at this time because there is a separate team evaluating the topic.

Q10. For Entities that are moving toward virtualized environments, will the SDT provide some guidance for those moving to it prior to the finalization of the revised standard? Alternatively, will there be a pilot implementation group similar to the V5 TAG pilot?

A10. The SDT plans to provide as much clarification as possible through guidance, outreach, and white papers. Many entities are already using virtualization in their environments and we will try to work with NERC to help provide a smooth transition.

Q11. What is SCI?

A11. Shared Cyber Infrastructure. It is a new definition to target requirements at the shared infrastructure on which virtual objects (machines, networks, and storage) execute (As depicted in grey in the drawings).

Q12. Does the proposed approach for the “shared infrastructure” categorization create a dual standard for compliance between data center (compliance at SCI) and substation environments (compliance at BCA level with ports and services and passwords, etc.)?

A12. The SDT plans to use the new term for Shared Cyber Infrastructure to target applicability within the standards.

Q13. From slide 27, how does the approach to 'deny all access to and from networks, with "networks" being the operative term, permit the use of a zero trust model. Doesn't this still prescribe the gated community model and preclude 'house'-level protections?

A13. The language on the screen was draft and we realize that it may not be the correct target for this requirement. We did want to share this approach with you for your consideration as we continue to draft better requirements.

Q14. How do you address the problem of VLAN hopping/crossover? Do you make a distinction between port based and logic based VLANs?

A14. To date, the SDT has been using the concept of logical isolation that can be created by various means including those you mentioned. The entity would be responsible to prove that their logical isolation is sufficient to meet the requirements.

Q15. Can you clarify the segregation requirements of shared storage? I understand the need for separate hosts for CIP and non-CIP assets - does that mean we need separate storage arrays or will logical access controls that segregate LUNs to hosts suffice?

A15. As we have been describing it so far, we would need to draft a new requirement targeted at the shared infrastructure to create logical separation. Those requirements are not yet complete.

Q16. Are there any lessons learned that will be delivered soon about those challenges?

A16. The SDT has been working on a model we call Pinecone Power, a fictitious entity that will be the foundation for guidance and future lessons learned whitepapers.

Standards Announcement

2016-02 Modifications to CIP Standards
Virtualization and Future Technologies: Case for Change White Paper

Informal Comment Period Open through June 28, 2019

Now Available

A 30-day informal comment period for the **Virtualization and Future Technologies: Case for Change White Paper** is open through **8 p.m. Eastern, Friday, June 28, 2019.**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. If you experience issues using the SBS, contact Wendy Muller. An unofficial Word version of the comment form is posted on the project page.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day.***

Next Steps

The drafting team will review all responses received during the informal comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual**.**

For more information or assistance, contact Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization and Future Technologies: Case for Change White Paper
Comment Period Start Date:	5/30/2019
Comment Period End Date:	6/28/2019
Associated Ballots:	

There were 30 sets of responses, including comments from approximately 84 different people from approximately 61 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the case for change based on the virtualization issues discussed in the white paper? Please provide comments.

2. Do you agree with the proposed path forward as discussed in the white paper? Please provide comments.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	1,3,4	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Public Utility District No. 1 of Chelan County	Davis Jelusich	1,3,5,6		Public Utility District No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Davis Jelusich	Public Utility District No. 1	6	WECC

						of Chelan County		
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Ginger Mercier	Prairie Power , Inc.	1,3	SERC
					Jennifer Bray	Arizona Electric Power Cooperative	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Patrick Woods	East Kentucky Power Cooperative	1,3	SERC
Duke Energy	Katherine Street	1,3,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC

Michele Tondalo	UI	1	NPCC
Helen Lainis	IESO	2	NPCC
Michael Jones	National Grid	3	NPCC
Sean Cavote	PSEG	4	NPCC
Kathleen Goodman	ISO-NE	2	NPCC
David Kiguel	Independent	NA - Not Applicable	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Gregory Campoli	New York Independent System Operator	2	NPCC
Caroline Dupuis	Hydro Quebec	1	NPCC
Chantal Mazza	Hydro Quebec	2	NPCC
Laura McLeod	NB Power Corporation	5	NPCC
Nick Kowalczyk	Orange and Rockland	1	NPCC
John Hastings	National Grid	1	NPCC
Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC

					Shivaz Chopra	New York Power Authority	5	NPCC
					Michael Forte	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC
Lower Colorado River Authority	Teresa Cantwell	1,5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE

1. Do you agree with the case for change based on the virtualization issues discussed in the white paper? Please provide comments.

Shirley Mayadewi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	No
Document Name	

Comment

We disagree with the case for change based on the virtualization issues.

In our view, except the Cyber Asset definition doesn't clearly include virtual machine, all the cases that are listed in the white paper can be addressed by the current Version CIP standards without significate changes.

The following are our assessments and suggestions for each case in the white paper:

1. Identification of Virtual Cyber Assets

We agree the current Cyber Asset definition doesn't include virtual machines explicitly. Given that any requirements apply to virtual cyber assets should as well as apply to physical cyber assets for the logical consistency, we suggest to modify the Cyber Asset definition to include virtual cyber asset rather than creating a new term "Virtual Cyber Asset", otherwise, the applicable system will become more complicated such as Virtual BCA, Physical BCA , Virtual EACMS and Physical EACMS, etc. We suggest modifying Cyber Asset definition as follows:

"A programmable electronic or virtual devices, including the hardware or virtual hardware, software, and data in those devices. Each virtual machine and host is a distinct device."

In addition, we suggest the hypervisor host should be identified as follows:

- the hypervisor host that contains one or more BCAs must be identified as a highest impact level BCA since it meets BCA criteria (deleting a BCA causes 15 minutes adverse impact).
- the hypervisor host that contains one or more EACMS must be identified as an highest impact level EACMS
- the hypervisor host that contains one or more PACS must be identified as an highest impact level PACS
- the hypervisor host that contains one or more BCAs, PCAs and EACMS must be identified as an highest impact level BCAs (high water-marking)

2. Distributed Firewalls vs. Perimeter Models

We haven't seen any challenges for applying current CIP requirements to this case. After VM falls within modified Cyber Asset definition, the Perimeter Model would apply to VM. If SDT thinks the ESP is not enough for the defense in depth and wants to add another layer network access control at an individual asset level (zero trust Model), it would become an expansion of CIP-005 requirements, which has nothing to do with virtualization. If it is allowable for individual VM to have high-level policy based network access control (zero trust Model) without designating perimeter level ESPs, the individual physical cyber asset should be allowable to do so as well (e.g., using local host firewall). In this case, CIP-005 R1.1 will be still applicable and CIP-005 R1.2 needs to be modified as follows for allowing device level network access control as an alternative measure:

“All External Routable Connectivity must be through an identified Electronic Access Point (EAP) or have network access control on each individual applicable Cyber Asset.”

Even though virtualization environments can force network access control at more granular levels including by user, process, or certificate and are not limited to only a source/destination IP address of a routable protocol, entities cannot get around the routable connectivity for the virtual networking. Regardless of virtual or physical network environments, routable protocols will be involved since only routable protocols allow devices to communicate between two different networks by forwarding packets between the two networks. Non-routable protocols only use a “device” address, and do not allow messages to be sent from one network to another, thus allowing communications to take place only on a single network. Note that Layer 3 protocols such as IP are often encapsulated in Layer 2 protocols such as Frame Relay, ATM (“Asynchronous Transfer Mode”), and MPLS (“Multiprotocol Label Switching”) for delivery of packets to distant networks. When such mechanisms are employed in Layer 2, the IP routable protocol is still in use. Therefore, the routable connectivity and ESP that have been used in current CIP standards are still correct and effective for addressing network access controls in a physical or virtual networking environment. Defining a new term ESZ is unnecessary since it cause more confusing and more unnecessary topology changes unless the project goal is for the defense in depth.

3. Virtualized Firewall Interfaces (‘Firewall on a Stick’)

We haven’t seen any challenges for applying current CIP requirements to this case. This switch with a firewall module can be addressed as follows using the current CIP requirements:

- For the layer 2 switch, If the switch is identified as a BCA, all (virtual and physical) devices are connected to the switch must be within an ESP
- For the layer 3 switch, the virtual firewall or the physical firewall module can be identified as a separate ECAMS containing EAP.
    - If the switch meets BCA criteria, it should be identified as a BCA, otherwise as an EACMS, where all non-BCA devices that are connected to the switch can be segregated by the above firewall.

  Given that the switch with a firewall module is not prohibited by the current CIP requirements, we don’t think the new asset classifications such as ESZ and SCI are needed.

    - 4. Virtual Storage Challenges

We haven’t seen any challenges for applying current CIP requirements to SAN. Also we disagree the SAN is only related to the CIP-011 information protection since SAN is normally used by a CIP Cyber Asset for the real time operations. Given that virtual or physical SAN like a local hard drive is used for the real time operations of a (virtual or physical) Cyber Asset; it must be treated as part of the Cyber Asset. For instance, if the Cyber Asset is a BCA, the SAN device must be identified as BCA and all BCA requirements would apply. If entities don’t want high-water marking the whole SAN as a BCA when the SAN is used in a mixed-trust environment, they should separate the non-BCA SAN for BCA SAN.

5. Management Plane Isolation

We haven’t seen any challenges for applying current CIP requirements to management plane. We disagree a shared cyber infrastructure classification is needed. The management plane device should be identified as part of CIP Cyber Asset it manages as follows:

- If the management plane device is used for creating, modifying, or deleting a virtual BCA, it meets BCA criteria (misuse causes 15 minutes adverse impact) and must be identified as a BCA.
- If the management plane device is used for creating, modifying, or deleting a virtual EACMS or PACS, it should be identified as an EACMS or PACS device. For clarifying this identification, we suggest modifying EACMS and PACS definitions to include the management devices as follows:

Modified EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes the Cyber Assets that can create, modify or delete the said Cyber Assets and Intermediate Systems”

Modified PACS: “Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. This includes the Cyber Assets that can create, modify or delete the said Cyber Assets.”

The concept of Figure 8 examples is wrong since BCA cannot be identified as an EACMS from the identification methodology perspective. In addition, if the management plane doesn’t meet BCA criteria, it would be a remote client and has to pass through an Intermedia System or identify the management plane itself as an Intermedia System.

6. Privileged Introspection

We haven’t seen any challenges for applying current CIP requirements to privileged introspection. After resolving the identification of Cyber Asset and management plane (see above), the current CIP-007 R3 already written at a security objective level and can work with privileged introspection seamlessly.

7. Remediation VLANs

We haven’t seen any challenges for dealing with remediation VLAN using current CIP requirements. As we described in Section 3), if the virtual firewall or the physical firewall module is identified as a separate ECAMS containing EAP, regardless of whether the switch is identified as a BCA or not, the remediation VLAN that is connected to the switch can be segregated from ESP since the remediation VLAN is not required to be within ESP by the current requirements if the remediation VLAN doesn’t contain any BCAs.

8. Multi-Site Data Center Extensions (Super ESP)

We haven’t seen any challenges for applying current CIP requirements to a super ESP. For the current CIP requirements, if a super ESP is designated across multiple geographic locations, all Cyber Assets within the ESP must be identified as BCAs or PCAs. If a primary control center to a backup control center across town or across the state, the Cyber Assets between two locations within a super ESP may be impossible to be managed as PCAs since some switches and routers may be owned by third parties. In this case, super ESP is not allowed by the current requirements and it is reasonable. Given that Protocol tunneling can explicitly bypass security restrictions and poses a serious challenge to network security, SDT shouldn’t modify the current CIP-005 requirements to allow use tunneling protocols between Control Centers within a super ESP without identifying in-between switches and routers as PCAs for protection.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	2016-02 Virtualization Review - RF Reveiw.docx

Comment

Note - please see attached word version as well as it has pitures which do not show up in this rich text box.

While the whitepaper provides some insightful thoughts on why change may be required, it is trying to create a solution for a problem that does not exist. This paper seems more of a proposal for allowing mixed-mode or mixed-trust environments as opposed to a need for change to accommodate virtualization. The term “shared infrastructure,” in the last paragraph in the Introduction section on page iv seems to hint towards a case for mixed-mode or mixed-trust environments. The term “shared infrastructure,” is not further documented or mentioned throughout the paper nor are it’s benefits communicated in the “Chapter 1: Virtualization Benefits” section. In addition to the concept of shared infrastructure, Figure 1 seems to leave out some critical layers of the conversion including the Hypervisor and network layers which is what logically and sometimes physically manages and connects the layers together as described in my proposed updated figure shown below.

Additionally, all of the benefits specifically listed in the “Chapter 1: Benefits of Virtualization,” section can already be used in the current CIP Standards just not used in a mixed-mode or mixed-trust environments. If all systems are high watermarked within the “shared infrastructure,” along with the proposed techniques and concepts being brought into scope, there would be minimal to no need for change.

Most entities audited to date in the RF footprint understand how a Guest VM should be categorized, with no changes to the current Standards or Requirements. As stated in the Guidelines and Technical Basis for CIP-005 – Electronic Security Perimeters (ESP) are required as a primary defense layer for those BES Cyber Systems (BCS) that may not have inherent cyber security functionality (such as relays, RTUs, or other physical Cyber Assets that would remain unprotected in some of the scenarios presented). In addition, the ESP provides clarity to determine what systems or Cyber Assets are in scope and what requirements they must meet. This does not preclude the use of a Zero Trust Model, but places the burden of compliance (and explanation at audit) on the Responsible Entity wanting to implement said model. Not only is there a burden of compliance, but also an additional burden of implementation and compliance with zero trust model technology on network, server, and security engineers and administrators.

For well over 10 years, most Microsoft, Linux, and Unix based operating systems have the ability to enforce zero trust models through built-in firewalls and application layer firewalls such as but not limited to:

- Microsoft Windows Firewall
- Ipchains
- ipfirewall
- iptables
- Netfiler
- nftables
- Anti-Virus/Anti-Malware vendor tools.

In many instances, these firewall services are disabled due to the complexity of:

- Troubleshooting network or application issues
- Changes in application network behavior from upgrades or patches
- Maintaining the additional amount of host based rulesets individually or through centralized management that would need to be assess per BES Cyber Systems and Cyber Asset.

-
- Whether zero-trust model tools as the ones described above, introspective versions done through a middle-ware layer in virtualization hypervisors, or 3rd generation switches/firewalls are used, these tools will not be a set-and-forget implementation. They will require regular tuning and maintenance, monitored closely through change management and require more documented elements to track and show for baselines and change management. Zero-trust models regardless of virtualization will greatly improve security and would be highly encouraged to do so, but it will require a high degree of monitoring, review, and constant tuning.
-
- Whether a zero-trust model and introspection tools are enforced or not, the underlying hardware supporting both the hypervisor and Guest VM are required for the operation of the Guest VMs, therefore it must be high water marked to the level of highest Applicable System impacted by the loss of associated physical hardware. This argument is the same for the hypervisor – without which the Guest VM cannot function or operate. Ultimately, minor changes to definitions to assist Responsible Entities in identifying and categorizing virtual devices would be beneficial, but not to the degree called for in the white paper and further cautions against mixed-mode and mixed-trust environments.

Many of the techniques and concepts described in the whitepaper are already allowable even though they are not specifically called out in the current standards or guidance. Many of the techniques and concepts could be used as above and beyond compensating controls for Technical Feasibility Exceptions (TFE)s and for Patch Mitigations. Noting these techniques and concepts as requirements for virtualization could preclude them from the use as TFEs and Patch Mitigations.

While virtualization is not specifically defined in the Standards, there is sufficient understanding between the Responsible Entities and CIP Auditors to set expectations and employ professional judgement to support the security of the BES at this time. Admittedly, virtualization will require minor changes in the current definitions to assist Responsible Entities with identifying Cyber Assets and their associated hypervisors and physical hardware, but not to the level outlined in the white paper.

Finally, RF noted that the white paper authors seemed to find extreme examples to include without noting more common layouts and examples that many Responsible Entities have already implemented. A suggestion would be to modify the current white paper to balance the examples presented with examples that Responsible Entities already have in place for further review and discussion.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	

As the question is overly broad, we will be providing comments broken down for the individual issues.

Identification of Virtual Cyber Asset – YES

PNM Resources agrees that there is a need to allow the Cyber Asset model to apply to virtual machines. There is also a need to identify the shared infrastructure the virtual machines need to function. Furthermore, the standards need to address when a machine has multiple CIP roles. For example, BES Cyber Asset that has only local accounts could also be considered an EACMS. If it has only local accounts is it not also preforming electronic access control? Or does the device high watermark to BCA? The current implementation guidance is not clear on this.

In addition to virtual machines the SDT needs to consider that technology is changing. Virtual machines are a decades old concept, but the standards are far behind at addressing. Today virtual applications or process virtual machines are also a reality. Depending on the implementation the virtual machine hosting the virtual application may be created from a template when the user calls on the application. The virtual machine is then destroyed when the application is closed. This mayfly virtual machine would have a hard time with the current CIP requirements. Yet this is a concept that virtualization allows and yet the white paper doesn’t address it.

Distributed Firewalls vs Perimeter Models – NO to the current reason

It is unclear as to why virtualization is driving this change. The white paper states, “This perimeter model is a prescriptive topology, and for many scenarios is still a valid way to perform network security. What may be prescribed, however, for a small network of similar cyber assets may not be ideal for a large network of virtualized BES Cyber Assets.” It doesn’t consider that it may not be ideal for even a large network of cyber assets. Virtualization may have a use case where the standard needs to allow for the distributed model, but the actual impetus for this is the current standard is overly prescriptive. It doesn’t allow for a defense in depth approach. Ideally entities would be using both the perimeter model and each host also protected with its own firewall. The white paper should make it clear that the current standard is preventing a more robust security approach that could apply to non-virtual systems. This is not a virtualization challenge in the NERC CIP Standards, but a challenge of overly prescriptive standards.

Zero Trust Models – NO to the current reason

The white paper does not make much of a case for change when it comes to the Zero Trust Model. Yes, the problem is that if a person gets past the community gate (EAP) and fence (ESP), then they could get into the house (Cyber Asset). This is not a problem with just virtual cyber assets, but physical cyber assets. It is unclear if a Zero Trust Model is required for only virtual cyber assets when physical cyber assets have the same problem.   Gated communities exist to provide a second layer of protection. The white paper doesn’t make it clear if this is an either-or proposition or if both will be allowed.

Virtualized Firewall Interfaces (‘Firewall on a Stick’) – NO to the current reason

Most of the problems such as the EAP conundrum in the Virtual Firewall Interfaces section are already covered in the Distributed Firewall vs Perimeter Models and Zero Trust Models and addressed by our comments in those sections. The more unique issue brought up in this section is regarding the question if the Network Switch is a BCS, EACMS or both. This concept is one that we have already discussed in our comments regarding Identification of Virtual Cyber Assets. This scenario highlights again that the standards are not clear regarding multi-role devices. Multi-role issues are not unique to virtualization. This is not a virtualization challenge in the NERC CIP Standards, but a potential gap in the current standards that impacts non-virtualized systems as well.

Virtual Storage Challenges – NO to the current reason

The white paper discusses challenges to virtual storage. The example of a Storage Area Network (SAN) or Network Attached Storage (NAS) array could very easily apply to a Redundant Array of Independent Disks (RAID). All entities should be utilizing a RAID on their BES Cyber Assets, so it is unclear why this challenge only comes up with virtual systems. It is unclear what this statement from the whitepaper means, “Additionally, there is no significant benefit to pulling drives from an array to sanitize or destroy them if there is another way to manage this media.” Is this saying that there is problem with CIP-011 when it comes to any disk array like a RAID. If so, does this mean that CIP-011 with regard to disposal or reuse should not apply to individual drives in an array? This is not a virtualization challenge in the NERC CIP Standards, but a challenge of overly prescriptive standards that impacts non-virtualized systems as well.

This topic also discusses de-duplication. This is not just an issue of virtualization. Many backup systems also employ de-duplication since many systems have similar information as described in the white paper. What happens to de-duplicated backups if all the BCAs are retired in a system upgrade, but some systems that share the de-duplicated data remain? Is the backup storage media still containing BCI or not? De-duplication is not just an issue of virtualization. This is not a virtualization challenge in the NERC CIP Standards, but a challenge of overly prescriptive standards that impacts non-virtualized systems as well.

Management Plane Isolation – NO to the current reason

The white paper discusses controlling access to the management plan of virtualized systems because they are logical constructs. However, this is not exclusively a virtualization issue. Many modern Cyber Assets that are servers or appliances have a baseboard management controller. This is the management plane of a physical server. If management plan isolation is an issue, then it an issue under the current standards for existing physical cyber assets. This is not a virtualization challenge in the NERC CIP Standards, but a potential gap in the current standards that impacts non-virtualized systems as well.

Privileged Introspection - NO to the current reason

While privileged introspection is a concept that does not have a physical corollary like some of the other concepts mention in Chapter 2, the paper fails to clearly identify the problem. The problem with “helper VMs” is that they have access to the entire kernel memory of the VMs they are monitoring. This kernel memory is “information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System." So, the "helper VM" contains BCSI. CIP-011 already requires procedures to protecting and securing handling BCSI including its storage, transit, and use. The "helper VM" is thus a designated storage location of BES Cyber System Information per CIP-004-5 R4.1.3., R4.4, and R5.3. This concept of a storage location isn't even in CIP-011-2, so the objective could be clarified in CIP-011-2 that storage locations of BES Cyber System Information needs to be identified. This is not a virtualization challenge in the NERC CIP Standards, but a potential gap in the current standards that impacts non-virtualized systems as well.

Remediation VLANs – NO to the current reason

The problem brought up in the white paper regarding adding a Cyber Asset under CIP-010 R3.3 is not unique to virtual systems. Virtual images can be physically moved from a non-production environment to the production environment using Removal Media just as a physical device is moved from non-production environment to the production environment. The concept of a remediation VLAN is misconstrued in the white paper. A limited VLAN with restricted network visibility can be setup for physical Cyber Assets so they can be assessed for vulnerabilities, update itself, and apply security controls to become compliant. The issue of the VLAN being inside the ESP or a separate ESP is the same. The remediation part only comes in when a machine becomes non-compliant and it is moved to the remediation VLAN. Any network switch utilizing Network Access Control can accomplish this.   This is not only possible with virtualization. This is not a virtualization challenge in the NERC CIP Standards, but a challenge of overly prescriptive standards that impacts non-virtualized systems as well.

Multi-Site Data Center Extensions (Super ESP) - YES

While the problem of Super ESP is introduced with a virtualization use case the reality is that the problem is anytime an entity stretches the layer 2 LAN across a WAN. At least the white paper in the last sentence of the section recognizes that the problem is not with virtualization, but prescriptive CIP standards that do not allow security measure that could achieve the security objective to be located somewhere.

Summary

PNM Resources does not see the challenges as being issues brought about by virtualization. Instead the problem is prescriptive standards that do not allow for other means to accomplish security objectives. Virtualization just happens to be the current technology that has revealed the prescriptive approach to cyber security is broken. It is to slow to change and the actual case for change is prescriptive standards don't allow for future methods to be easily applied and remain compliant. The standards drafting process is too slow to keep adjusting every time best practices for cyber security change. The white paper is "Virtualization and Future Technologies" yet future technologies is only referred to once in the document. The issue isn't even virtualization. The problem is the standards have prescribed best practices as a particular point in time. However, technology of how tasks are done is changing and with it is the technology of how to secure it. What isn't changing as much are the objectives of security which is discussed more in response to question #2.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3,5

Answer	Yes

Document Name	
Comment	
AEP supports the efforts of the SDT to change or add definitions and requirements related to the application of virtualization technology to an objective level; making the language describe “what” is required not “how” it is to be implemented. The danger is that the requirement language may be too broad thereby adding to the compliance burden and making compliance assessment more difficult or; too specific such that it excludes viable security solutions. AEP requests the SDT take the time necessary to find that “just right” language that creates the desirable outcomes and avoids unintended consequences.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA concurs that the current model does not cover virtual cyber asset requirements.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes

Document Name	
Comment	
Reclamation supports modifications to the CIP standards to future-proof the standards and allow for changing technologies. The proposed approach will benefit industry by allowing entities to achieve compliance while protecting their BES Cyber Systems regardless of the composition of the BCS. Reclamation supports a less prescriptive and more objective-based security framework that allows entities to define their systems at the level that makes sense for a situation. Reclamation recommends the SDT clarify the usage of “(compute, network, storage)” on page 3 of the white paper. Reclamation also recommends a more thorough quality review of the white paper to correct typographical errors throughout the document.	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
CHPD agrees with the case and appreciates the thorough explanation provided by the SDT.	
Likes 0	
Dislikes 0	
Response	
Line Dufour - Hydro-Qu?bec Production - NA - Not Applicable - NPCC	

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

Idaho Power agrees there is a need for virtualization. The current CIP standards don't translate well to current uses of several valuable technologies that include those that rely on virtualization.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	Yes
Document Name	

Comment

N&ST considers it reasonable to calll attention to virtualization's potential benefits, but only up to a point, and we consider the WP's negative comments about many current CIP implementations (e.g., Fig. 4 "Perimeter Based Model" is characterized as "Not aligned with current security best practices") to be needlessly pejorative. Moreover the WP:

- makes several assertions that N&ST considers inaccurate, such as the suggestion that multi-site ESPs and the current Standards are incompatible,

- pays fairly little attention to the issue of how compliance with current or modified CIP Standards could be demonstrated, and

- does not directly address the question N&ST believes entities have found most nettlesome, which is whether it is allowable for CIP and non-CIP VMs, managed by a single hypervisor, to coexist on a shared hardware platform and, if so, what conditions would have to be satisfied.

These concerns notwithstanding, N&ST agrees with the WP's main premise, which is that the Standards, along with several current definitions such as "Cyber Asset," should be updated to accommodate entity implementations that are partially or even entirely based on virtual systems. N&ST also strongly supports the goal that any and all revisions should be developed in a manner that fully supports "backward compatibility" and does not compel entities with no major technology updates on their planning calendars to revise their existing set of CIP policies, plans, and procedures.

Likes 0	
Dislikes 0	

Response

Neil Swearingen - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI member companies generally agree that the SDT has provided a clear and concise case for change based on the virtualization issues identified within their white paper. We recognize that steps need to be taken to provide a path forward for those entities that see reliability and security benefits in virtualization technologies while not disrupting the compliance programs of others. EEI appreciates the direction described in the white paper and support the SDT's current, more moderate approach, which we believe will better ensure broader industry acceptance of the changes being proposed. However, more work is needed to identify the security risks associated with virtualization and address methods to mitigate those risks to ensure continued BES reliability and security. We also note that while cloud computing is not directly addressed in the white paper, the document should be clear that the SDT's approach is not seeking to enable the use of off-premise third party cloud platforms for BES system operations (e.g., Supervisory Control and Data Acquisition (SCADA)).

EEI member companies would also like to take this opportunity to commend NERC and the SDT on the proposed direct described in the white paper while also encouraging NERC's long term objective of transforming the NERC CIP Reliability Standards into a body of standards that more closely conform to the results-based standards concept that currently drives all other NERC Reliability Standards. Still, EEI believes that the drafting team has selected the right path for this current effort.

Likes 0	
Dislikes 0	

Response	
Barry Lawson - National Rural Electric Cooperative Association - 3,4	
Answer	Yes
Document Name	
Comment	
In the white paper, and Q9 in the Q&A document, it’s unclear whether the SDT is treating a Storage Area Nework (SAN) as a separate BES Cyber Asset (BCA) or only as a BES Cyber System Information (BCSI) storage location. NRECA requests that the SDT clarify this going forward. NRECA recommends that the SDT be congnizant of the layering that can occur through virtualization, especially if the CIP requirements are already applying to the hardware. In this situation, any new requirements applying to virtual devices on that hardware should be limited or non-existent. The current CIP standards are unclear as to whether a programmable electronic device definition can exclude a virtual machine. NRECA recommends that the SDT take this into consideration while drafting new or revised requirements.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
We agree with the case for change for virtualization and classification of such assets. The suggested changes will allow entities to be much clear in classifying a Cyber Asset.	
Likes 0	
Dislikes 0	
Response	
Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC	
Answer	Yes
Document Name	
Comment	

NCEMC Agrees with the comments submitted by NRECA

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

Seattle City Light finds the white paper to be an excellent summary of the technological evolution in virtualized systems and the challenges the standards drafting body faces in updating the standards to accommodate that evolution. We were very impressed by how well the technical concepts of virtualization were described for a non-technical audience and how they were cross-referenced to the existing physical asset-centric approach of the current standards.

The Q&A document illustrated that, as good as the white paper was, there is still work to be done to help the industry not lose sight of the forest for the trees.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

ERCOT requests that the SDT make clear whether the implementations referenced are for on-premises solutions only. If the intent is to include cloud provisions, that should be articulated specifically. There is a lot of dispute about cloud solutions for BES Cyber Systems and other asset types subject to NERC CIP Standards that may not make this the right venue to address and achieve a timely solution as noted in the paper. More concrete work is needed by NERC related to cloud services before it is appropriate to include those issues.

Many of the concepts documented in the paper also apply to physical systems. The paper points out some significant vulnerabilities with current implementation. ERCOT requests that the SDT look at these issues as well as the virtualization issues to ensure that gaps are addressed with legacy systems.

Likes 0	

Dislikes 0	
Response	
Katherine Street - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Systems and technologies supporting Control Centers, where IT-based solutions are prevalent, are rapidly evolving beyond concepts that are foundational to the current NERC CIP Reliability Standards. Multiple vendors have indicated intentions to fully virtualize their offerings in the next few years, and hardware suppliers are hinting that the traditional rack-mount physical server will no longer be an option in the future. The SDT's case for change focuses on virtualization, but the concepts discussed apply to future-proofed network technologies that provide higher resiliency and flexibility for critical communication flows and to server hardware as it becomes hyper-converged with multiple individually-programmable components inside. The NERC CIP Reliability Standards must evolve to support these technology advances. Although some lag behind bleeding edge tech is expected regulatory standards should not preclude the use of resources that are generally available and meet security objectives, such that entities are forced to turn to grey-market sourcing in an effort to obtain compliant resources.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE appreciates the standard drafting team's (SDT) effort to align the NERC Reliability Standards within the current technology. Texas RE agrees with the following concepts described in the white paper:	

- Identification of Virtual Cyber Assets: Texas RE believes providing clarity on how to identify and categorize Virtual Cyber Assets to ensure consistency across all regions would be beneficial for the industry.
- Virtual Storage Challenges: Texas RE agrees that with the proposed changes to CIP-011-2 R2 there may be difficulties proving compliance in a virtualized storage environment.
- Remediation VLANs: While it is technically possible to comply with CIP-010-2 R3.3 in a virtualized environment Texas RE recognizes that additional clarity on how to deploy this technology in a secure and compliant manner would benefit the industry.

The white paper appears to argue that certain components of virtualization are not possible due to the way the standards are written. While Texas RE agrees there could be additional clarity and specific mention of virtual machines, nothing prevents entities from implementing the following:

- Distributed firewalls: Perimeter controls would also need to be deployed to meet CIP compliance, however this existence of perimeter controls does not prevent entities from deploying additional controls.
- Zero Trust Models: Perimeter controls would also need to be deployed to meet CIP compliance, however this existence of perimeter controls does not prevent entities from deploying additional controls.
- Management Plane Isolation: Entities are capable of deploying secure management plane communications today.
- Privileged Introspection: CIP-007-6 R3.1 states “Deploy method(s) to deter, detect, or prevent malicious code.” An entity using privileged introspection would only need to document that this is their method of deterring, detecting, or preventing malicious code. The SDT also stated that this technology would require grouping VM’s protected by privileged introspection into a particular BES Cyber System. Texas RE is unsure why the SDT believes this to be the necessary.

Texas RE suggests that the discussion surrounding Multi-Site Data Center Extensions (Super ESP) is applicable to all Super ESPs, and is not a change specifically necessary for the standards to be able to successfully address virtualization.

Additionally, Texas RE is concerned with a mixed-trust environment. Due to the parent child relationship between host and virtual machine, you can never fully eliminate impacts a VM could have on other VM’s and the host.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion

Answer	
Document Name	

Comment

At the executive level – 1) Expect the SDT to provide virtualization benefits; 2) Request the SDT also provide virtualization challenges – operational, cyber security and compliance.

We are concerned that moving to “security objectives” will significantly impact auditors, starting with their training.

Chapter 2 is an excellent start to the conversation of challenges in moving CIP to a virtualization

Likes 0	
Dislikes 0	

Response

2. Do you agree with the proposed path forward as discussed in the white paper? Please provide comments.

Trevor Tidwell - PNM Resources - 1,3 - WECC,Texas RE

Answer	No
Document Name	

Comment

The path forward should be more requirements focused on an objective and meeting that objective. Allow the entity to define how it is meeting the objective, so that it can be changed as security technologies change, but the objectives generally do not change as much over time. New threat vectors may arise and necessitate a change to the standards to add a new objective, but that is easier to achieve than rewrite the prescription on how to stay compliant.

The reason for the no vote is for two reasons. The first is that the proposed path forward isn't entirely clear. While the whitepaper appears to be suggesting that the path forward is more objective than prescriptive, it is short on detail. It gives only one example and would be better off with a couple of more if the intent is to truly move to objective level rather than prescribing the method of meeting the objective. In a world of Advanced Persistent Threats, we need to move to an objective model. While the threats are persistent, they are not static. Industry best practices typically are our defense playbook. These threats adapt to the playbook and find new ways defeat it. As a result, technology and practices used by industry change in response. Yet the security objectives remain the same, but the means of doing so have changed. Writing the NERC CIP Standards to mimic today's best practices do not allow industry to have the ability to adapt when those practices change. As a result, Entities are potentially more exposed to a threat because a new security method doesn't fit the prescription imposed on it. Technology is always changing and writing a prescription for security methods today and attempting to look to the future is a fool's errand. We cannot image today what technology will be like in 5 to 10 years. However, we can foresee what the security objectives are. It is much like war where the objectives are the same, but over the centuries the tools of warfare have greatly changed how you achieve those objectives.

The second reason for the no vote is that the current path forward does not address defense in depth. For example, if an entity implemented both a perimeter and distributed firewalls and had a failure of a perimeter control, but all the devices in the ESP had some compensating control that mitigated the risk of the failure then that should not be a violation of the standards. While one method of achieving the security, objective failed another remained in place. This would help encourage defense in depth if entities could have multiple controls that met the security objective if they could also mitigate risk of non-compliance. To be clear this would be multiple independent controls capable of meeting the security objective where failure of one doesn't result in failure of the other. It is not saying that an entity could have many controls with interdependency of meeting the security objective where a failure of one control results in a failure to meet the objective.

In summary, PNM Resources would encourage the drafting team to think of what the objectives are then rewrite the standards with those in mind. Do not try to keep the current framework as it is broken when trying to adapt to new technology. While this effort discusses virtualization, the reality cloud computing has resulted in a new effort on CIP-011. Thus, the current prescriptive paradigm needs to move to an objective paradigm where an SDT isn't formed with every new emerging technology. We would encourage the SDT to develop this new framework then map the old requirements to the new objective-based framework. Not everyone may appreciate another major paradigm shift with CIP. However, if the SDT can put out a good draft product of revised standards and framing it as more objective standards and less prescriptive standards are the right way to go, then the rest of the industry will hopefully agree. The SDT needs to stop framing this as a virtualization problem since many are already virtualized under v5. The problem is overly prescriptive standards preventing Entities from being able to change the methods of accomplishing the security objective in a compliant manner.

Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

While there may be some credence to modifying the definitions of what a BES Cyber Asset is to better accommodate virtual environments (see discussion above), for the most part, the Responsible Entities that RF audits correctly identify and protect Guest VMs, hypervisors, and supporting physical hardware. The Responsible Entities do not identify Guest VMs as “software” but as BES Cyber Assets, Protected Cyber Assets (PCA), or BES Cyber Systems (BCS). RF does not agree that Guest VMs are specifically excluded from the current CIP-007 Requirements as stated in Figure 2 on page 3.

Admittedly, there is a 1:1 relationship assumed between BES Cyber Assets and their underlying hardware, however, minor changes to current definitions will support one-to-many relationships afforded in VM environments without creating new asset classes.

The argument put forth under “Distributed Firewalls vs. Perimeter Models” on page 4 is already possible as mentioned above. Entities can choose to identify and protect each BCA in their own separate ESP, with their own separate EAP, under the current CIP Standards. While virtualization may reduce the amount of time and effort to implement such an environment, maintaining it with a high degree of confidence that it is performing as designed, and then explaining this environment to an outside auditor could prove challenging.

Further, current “Next Generation” firewalls are fully capable of limiting network access into and out of the ESP across most layers of the OSI model through security zones. Figure 4 compares Perimeter-based and Zero-Trust models, and as most Cyber Assets use the same LDAP or Active Directory (AD) access, the Zero-Trust model is not as secure as portrayed – unless there is the same granularity implemented within the AD or LDAP environment for Groups or ACL Sets and incorporated in the Guest VMs security group.

Remediation VLANs, as shown in Figure 10 on page 10, would be considered “above and beyond” the CIP Standards and would earn a Responsible Entity a Positive Observation, showing strong internal controls for patch management and malware detection.

RF already identifies Super-ESPs (mentioned on page10) and has multiple entities that have currently implemented and support these extended ESPs. There are no additional requirements or changes required for this to be implemented.

Best practices support rings of security in a “defense-in-depth” model that creates tighter security controls the closer you get to key systems. Access control applied at deeper levels as described within the white paper on page 13 does not require virtualization, but at the discretion of the Responsible Entity can be done through a combination of firewall rulesets or security zones, intelligent switches with ACLs or zones, host firewalls, Group Membership (AD), ACL Sets (LDAP), and individual Cyber Asset malware detection.

Regardless of what the paper calls “Shared Infrastructure,” there does not need to be new asset classes, as any new asset classes would still require identification at the high water mark to the level of highest Applicable System the Cyber Assets are controlling access within a distinct ESP. CIP definition changes to include “per device capability” would allow leeway for the auditors to have a conversation and draw conclusions based on professional judgment based on the story the Responsible Entity tells.

Conclusion

RF as a region supports virtualization; however, all supporting hypervisors and underlying physical hardware must be included and categorized correctly. Much in the same way that a network switch within the ESP cannot operate in mixed-mode, neither can Guest VMs that are categorized as PCA, BCA or part of a BCS operate in a mixed-mode environment with non-CIP Guest VMs. Only those Applicable Systems outside of the identified ESP – PACS and EACMS – may operate in a mixed-mode environment; and the underlying hypervisor and physical Cyber Assets must be protected as either a PACS, EACMS, or both – if both are running as Guest VMs.

Using virtualization completely within the ESP – or outside of the ESP for EACMS and PACS – leverages virtualization and captures many of the benefits while limiting the changes required to meet current or future CIP Standards and Requirements.

Likes 0	
Dislikes 0	

Response

Shirley Mayadewi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	No
Document Name	

Comment

We disagree with the proposed path forward as discussed in the white paper. In our view, current CIP requirements can apply to virtualization environment smoothly without significant changes. Given that the CIP compliance program today works fairly smoothly by implementing the existing requirements, any changes of requirements and definitions beyond virtualization shouldn’t be targeted. SDT should focus on how to resolve CIP compliance in the virtualization environment without prohibiting the new technology rather than try to change the requirements for the defense in depth since it is not the driver for this project. Resulting from our comments in the above question 1, as long as the Cyber Asset definition are modified to include VM, most of existing CIP V5 requirements would apply to virtualization environment seamlessly.

Likes 0	
Dislikes 0	

Response
Teresa Cantwell - Lower Colorado River Authority - 1,5, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

The path forward is needed. However, two items are of concern from this statement:

A literal use of this foundational definition would mean a server hardware platform may be a BES Cyber System, the hypervisor software could be the "operating system", and all the virtual machines running on the hardware are applications or simply data.

1. It should be clear of the differences between an operating system and an application. NIST provides the following definitions.

Operating system: A computer program, implemented in either software or firmware, which acts as an intermediary between users of a computer and the computer hardware. The purpose of an operating system is to provide an environment in which a user can execute applications.

Application: A system for collecting, saving, processing, and presenting data by means of a computer. The term application is generally used when referring to a component of software that can be executed. The terms application and software application are often used synonymously.

The OS can prevent or allow the application to run, but not necessarily vice versa. A clear hierarchy is created. The hypervisor is then above both the OS and application for each VM instance and holds primary control. Therefore, it is recommended that changes to the CIP Standards have three clear tiers when addressing virtual environments to include 1) hypervisor, 2) VMs and OSs, and 3) applications. VMs/OSs and applications should not be grouped together.

2. With all the current discussions on BES Cyber Information and controls used to protect it in cloud environments, the SDT should use caution when using the word "data". Data is not useable until it is information. The SDT may have the opportunity to also address this issue as encryption, where information is turned to data, may be used in virtual environments.

Likes 0	
Dislikes 0	

Response
Katherine Street - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

The path forward is reasonable given that current popular uses of virtualization technologies do not provide substantial direct benefits to many of the field systems that must comply with the NERC CIP Reliability Standards. Nonetheless Reliability Standards drafters, Registered Entities, Compliance

Auditors, and other stakeholders must have clarity and regulatory certainty regarding how newly proposed defined terms function in relation to current NERC Glossary of Terms Used in Reliability Standards definitions. The questions noted in the White Paper with respect to the Shared Infrastructure's possible 15-minute impact are indicative of the questions that will arise if the standards do not clearly address how to classify a given "asset" when multiple definitions align with that asset's function. Of particular concern is Shared Infrastructure supporting exclusively EACMS and PACS devices. There is no 15-minute impact question in this scenario, but if the Shared Infrastructure definition assumes a need for BCA-level protections, entities will be forced to add protections not otherwise anticipated for those environments. Similarly, the NERC Reliability Standards must provide Compliance Auditors and Registered Entities clear parameters for assessing regulatory compliance where Shared Infrastructure supports Virtual Cyber Assets that would be classified differently under current rules. For example, would a virtual BCA and virtual PACS be allowed to reside on the same Shared Infrastructure with different network protections deployed (one requiring an "ESP" and one not)? We support the SDT's efforts to develop the new NERC Glossary of Terms Used in Reliability Standards definitions, and look forward to working through these complex issues to arrive at a sustainable approach compatible with evolving technologies.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

Virtualized Firewall Interfaces: ERCOT questions whether the use of the term "firewall" is too specific. More generic terms should be used to allow for other device types that provide this security capability. If the concept of an EAP is maintained, this could result in a one-to-one definition of EAP to Cyber Asset. ERCOT requests consideration of how to define the access points without too much of an administrative burden.

Management Plane Isolation: ERCOT requests that "per asset capability" be included and added to requirements related to management plane isolation.

Multi-Site Data Center Extensions (Super ESP): ERCOT requests that any future requirements related to this subject be aligned to complement and not conflict with or extend the requirements of CIP-012.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

Seattle City Light generally agrees with the proposed path forward. In particular, we like the direction headed with the new “no trust” model.

We remain concerned about maintaining backward compatibility with existing CIP standard language and terminology, and encourage that, at least in certain cases (if not throughout all CIP requirement), the SDT consider use of “overlay” requirement language that accommodates virtualization approaches while also maintaining existing language and terms (i.e., give an entity the option to choose between the existing requirement—perhaps revised to focus on risk and result rather than prescriptive approach—and a new, alternative requirement for a virtualized system. This option would exist on a system-by-system basis).

We also are concerned that the virtualized shared storage (SAN) concepts require a closer look, in terms of treatment under CIP requirements. This area might be ideal for use of the virtualization “overlay” approach discussed above.

Likes 0	
Dislikes 0	

Response

Kagen DelRio - North Carolina Electric Membership Corporation - 3,4,5 - SERC

Answer	Yes
Document Name	

Comment

NCEMC Agrees with the comments submitted by NRECA

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion

Answer	Yes
Document Name	

Comment

Our concern is that although the example (figure 12) follows the model given it does not represent the complexity under which the industry has implemented CIPv5

We request the SDT post updates to CIP-007 and CIP-010 sooner. Those Requirements are the biggest hurdles. The industry and SDT will quickly see if the new Requirements will be acceptable

We support the proposed creation of new “shared infrastructure” and “virtual machine” cyber asset types and new “objective-based” type requirements specifically for those virtual cyber assets (as per Chapter 3) which would allow entities to adopt virtualization incrementally and at their discretion without changing existing CIP programs for entities that choose not to adopt virtualization.

We request the SDT to describe how they plan to address mixed-use environments (hardware resources shared between CIP and non-CIP virtual machines)

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

While we are in favor of the proposed path forward, we feel like there is not enough evidence zero trust, software defined networking, and or other similar technologies are more reliable, less expensive, easier to manage, and provide better security in real-time controls networks ie: SCADA, DCS, ICS. These cybersecurity tools have been developed for rapidly changing IT envrionments and for highly exposed, high risk Cyber Assets. BES Cyber Systems are neither of those.

We feel the SDT should focus on the changes to virtualization in the two first bullet points in the whitepaper’s conclusion and let the “Virtualized Network” security product industry mature before changing the standard. We realize the standard is prescriptive in it’s nature around electronic border security, but does not preclude an entity from using other technologies to protect Cyber Assets discussed in the paper such as Management Plane Isolation, Privileged Introspection, etc.

Border firewalls are still considered a best practice and the cost of having a border firewall should not be considered “purchasing extra hardware to show compliance with prescribed technologies”. Firewalls are still a corner stone of protecting networks against attacks and modern firewalls are no longer confined to layer 3 of the OSI model. The standards require and EAP, but that does not preclude an entity from employing more protective and restrictive controls than the standard requires such as Next Generation Firewalls which operate up to Layer 7 of the OSI model and integrate with Identity and Access Management controls. If FERC and or NERC feel the modern threat landscape requires more granular controls then new requirements are warranted.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 3,4

Answer	Yes
Document Name	

Comment

NRECA appreciates the efforts of the SDT in addressing the complex but important issue of virtualization in the CIP standards.

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation

Answer	Yes
Document Name	

Comment

We do like the initial path that you have discussed and would like to see more information on:

a. direction and clarification on the Shared Storage and Shared Networks

b. examples of “access control at a deeper level”

Also, the webinars that were put together have been very helpful. We encourage you to continue to use them as an informative tool to illustrate your plan.

Finally, we feel it is important to reiterate that if an entity does not elect to leverage virtualized technologies, then they should not need to alter their programs at all to maintain compliance to any of the CIP requirements.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the path forward as described in the Virtualization white paper, which aligns well with EEI comments provided in December 2018 to the SDT. As stated in those comments, EEI urged the SDT “to focus more on how virtualization might be effectively integrated into BES Cyber Systems, under the current standards, rather than trying to solve all these issues at an early stage of industry adoption.” As a result, we are encouraged by the proposed concept as described but also recognize that much work remains, conceding that many of the concepts will need to be developed in greater detail and vetted by the industry. However, we believe that the SDT has proposed a concept that EEI member companies can support and look forward to reviewing and providing comments that align with the direction described in the white paper.

Likes 0	

Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
N&ST recommends the frequent involvement of representatives from Regional Entity Compliance Monitoring and Enforcement groups, as audit approaches for virtualized CIP environments are likely to be significantly different than for non-virtualized environments.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Idaho Power believes the proposed path forward appears to be an appealing approach. However, due to the amount of significant changes that will occur as a result of this approach, it appears that the proposed path forward could result in significant increases to a Responsible Entity's overhead costs and associated resources. In addition, when any newly approved CIP standard becomes effective, Responsible Entities require long lead times to plan, interpret, document, and implement changes into their compliance programs and processes in order to have a suitable and sustainable compliance program associated with the new CIP standard. At minimum, a 24-month implementation plan should be considered.	

Likes 0	
Dislikes 0	
Response	
Line Dufour - Hydro-Qu?bec Production - NA - Not Applicable - NPCC	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
CHPD supports the proposed concept to include new language that specifically scopes virtual environments as an extention to the existing standards, while maintaining compatibility with the compliance approach used now for existing non-virtual systems. CHPD requests that the SDT consider developing language that is more specific and reduces the potential for scoping confusion. For example, the proposed Management Plane Isolation change could be written to ensure that only applicable virtual hosts (e.g., those hosting BCAs, EACMS, etc…) and their associated hypervisors are considered under new requirement language. This approach would prevent other CIP asset types like BCAs or PCAs from being unintentionally included.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	

1. In reviewing the comments on the Q&A, it’s unclear as to whether the drafting team is treating a SAN as a separate BCA or only as a BCSI storage location. Could the SDT please clarify?

2. Seminole recommends the SDT to be cognizant of the layering that can occur through virtualization in that if CIP Requirements are already applying to the hardware that Seminole would prefer that the additional Requirements applying to the virtual devices on that hardware would be limited or non-existent.

3. The Standards are unclear as to whether a programmable electronic device definition can exclude a virtual machine. The SDT should take this into consideration while drafting revised Requirements.

Likes 0	
Dislikes 0	

Response

Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6

Answer	Yes
Document Name	

Comment

No Comments

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	Yes
Document Name	

Comment

Reclamation supports the SDT’s intent to create security objective-based requirements; however, the Case for Change White Paper seems to be addressing virtualization at too granular of a level. Many of the challenges and scenarios discussed are hypothetical, extremely detailed, and appear to require extremely detailed and complicated CIP requirements. Reclamation is concerned that the path forward as described will result in requirements with a compliance/documentation burden that is not commensurate with the level of risk reduction provided.

Reclamation recommends the SDT incorporate virtualization into the CIP standards by clearly identifying and defining the scope of what must be protected while retaining the language in the current versions of CIP standards. For example, a requirement might state that entities are required to protect against unauthorized access to BES Cyber Systems. To address this existing requirement for both virtualized and non-virtualized environments, Reclamation also recommends the SDT revise the definitions in the NERC Glossary of Terms to include virtualized systems and leverage the existing

requirement to protect against unauthorized access. Reclamation does not support creating a virtual counterpart definition for all existing physical definitions. Definitions should include physical and virtual aspects of the defined terms.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA concurs with the path forward, but "shared infrastructure" qualifications would need to be defined since this will be a new asset class. The standard should be as specific as possible to highlight the difference from existing hardware.	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3,5	
Answer	Yes
Document Name	
Comment	

AEP requests the SDT include sufficient flexibility to allow entities to transition from their current compliance strategy to a newly available strategy and remain compliant throughout the process. Further, AEP requests the SDT make any new or revised requirement language backward compatible to the current obligation for systems not affected by virtualization. AEP believes there should not be a cost to entities that results from changes made to requirements and definition to accommodate virtualization technology.

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE noticed that the SDT seems to have gone outside the scope of the 2016 Standard Authorization Request (SAR). Texas RE inquires as to whether a new SAR should be submitted.

The 2016 SAR states “Virtualization – The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider CIP-005 and the definitions of Cyber Asset and Electronic Access Point regarding permitted architecture and the security risks of network, server and storage virtualization technologies.” Modifying the CIP standards to embrace new security techniques is not an issue that was included in the V5TAG Transfer Document nor was the SDT instructed to address issues with the standards’ adaptability to current and future technology innovation.

While Texas RE agrees that some changes should be made to the CIP standards, not all of the changes are necessary at this time, nor are all of the changes specific for virtualization.

Texas RE recommends the following path forward:

- Modify the Cyber Asset definition to include virtual machines, hosts, etc.
- Create a separate standard for virtualized environments or modifying CIP-005-6 to include security objectives for virtualized environments.
- Not making any changes to the ESP and EAP terms as they are defined broadly enough to give entities the flexibility in how they apply those terms within many types of network architectures.

Likes 0	
Dislikes 0	

Response

Virtualization and Future Technologies: Case for Change White Paper Consideration of Comments

Project 2016-02 Modifications to CIP Standards

The Project 2016-02 SDT (SDT) developed the "Virtualization and Future Technologies Case for Change" White paper to explain the need to change the cyber security CIP Reliability Standards. This white paper has not been approved or endorsed by NERC and solely includes the views of the SDT.

Recognizing the continuing growth in technology innovation, many entities in the Electricity Sector have implemented virtualization as part of their CIP programs. Many of these same entities, however, have implemented this new technology without taking full advantage of virtualization's advanced capabilities. There are several reasons for this from the constraints of the current CIP architecture to the ongoing ambiguity around how new virtualization technology applies to CIP compliance. Some of those who are implementing virtualization are experiencing a great deal of uncertainty and difficulty around developing implementation strategies that will support compliance and achieve greater reliability and security. The SDT was assigned the task to address the technological innovation in virtualization within the CIP standards.

The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards. The SDT's intent is to better position the CIP standards to be applicable to any future technological innovation. Leveraging the abstraction that virtualization provides will allow the industry to more readily adopt new technology and increase security posture. This paper presents the SDT's case for change to the NERC CIP standards that is needed to allow for the innovative security techniques and new concepts brought about by virtualization.

The SDT thanks the industry for its time and attention to these matters and the resulting comments. The more popular, overall themes from the comments received have been captured and considered in this report, in order to progress towards a formal posting.

Overall Themes

- **Commenters were unclear as to how the SAN would be classified and treated.** The Standards Drafting Team thanks you for your comment. The SDT contends that due to nature of the overall configuration of traditional SANs (i.e. non-IP transport protocols, data de-duplication, volume spanning across multiple drives, etc.), that this is better addressed as part of a future change to CIP-011. The SDT is considering how to address CIP-005 issues with non-IP based protocols typically used in SANs. Please refer to the forthcoming CIP-005-7 Technical Rationale for Requirement R1.5.

- **Commenters were concerned regarding double jeopardy if both the virtual machine and the host are cyber assets.** The Standards Drafting Team thanks you for your comment. The SDT contends that the physical equipment that is hosting Virtual Cyber Assets should fall within the proposed new Shared Common Infrastructure (SCI) definition. The SDT will consider this situation while drafting the next version of the standard.
- **Commenters questioned if programmable electronic devices exclude a virtual machine.** The SDT thanks you for your comment. The NERC Glossary definition of Cyber Asset has a direct tie to the hardware on which it relied. This affected the definitions of the "Applicable Systems" terms such as BES Cyber Systems (BCS), EACS, PACS, and Protected Cyber Assets (PCAs). Because the Reliability Standard is applicable to the systems, the control for the Cyber Assets also applies to the hardware. This tie to hardware implies a singular one BCA, EACS, PACS or PCA per individual hardware system. This singularity is what virtualization intentionally breaks to increase reliability, and resiliency.

  The proposed NERC Glossary definition of Virtual Cyber Asset (VCA) and ESZ allow the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined. The VCA definition references a newly defined term, Shared Cyber Infrastructure (SCI) that does not include hardware. The definition of VCA is not inclusive of hardware, and the EACS, PACS and PCA definitions have been updated to allow for VCA versions. With the addition of SCI and revisions to the "Applicable Systems", there can be one or more virtualized instances of a BCA, EACS, PACS or PCA that reside on a single SCI.
- **Commenters were concerned with cloud services.** The SDT thanks you for your comment. At this time, the changes that the SDT have proposed are intended to better futureproof the standards for the use of the same virtualization technologies that cloud providers use, but for in-house (on-premise) system. While this sets the stage for facilitating future considerations such as the use of cloud providers, the SDT is not addressing the hosting of BES Cyber Systems with off-premise cloud providers at this time.

  The SDT notes that at some later date, it will be making conforming changes in the CIP Standards in collaboration with the NERC Project 2019-02 BES Cyber System Information Access Management SDT.
- **Commenters were concerned about the technological advances that are occurring and the desire for standards to evolve to accommodate these developments.** The SDT thanks you for your comment. At this time, the changes that the SDT have proposed are intended to better futureproof the standard to reduce the number of changes required as technology evolves. The SDT contends that while futureproofing the standards for future technological changes is desirable, this must be balanced against the need for backward compatibility to exist where possible.
- **Commenters expressed that regulatory standards should not preclude the use of resources that are generally available and meet security objectives.** The SDT thanks you for your comment. Project 2016-02 SDT was assigned the task to address the technological innovation in virtualization within the CIP standards. The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards. The SDT's intent is to better position the CIP standards to be applicable to any future technological innovation. The SDT agrees that the standards should be

flexible to meet security objectives with currently available resources and not prescribe technologies or architectures.

- **Commenters expressed that changes should apply to both physical and virtual devices.** The SDT thanks you for your comment. At this time, the changes that the SDT have proposed are intended to better futureproof the standard to reduce the number of changes required as technology evolves. The SDT contends that while futureproofing the standards for technological evolution is desirable, this must be balanced against the need for backward compatibility to exist where possible. This need for backwards compatibility may limit the number proposed changes possible to physical devices.
- **Commenters were concerned with problems related to multi-role devices not specific to virtual devices.** The SDT thanks you for your comment. The SDT intends to address of the possibility that Cyber Assets may fall within multiple classifications (i.e. simultaneously be both SCI and PCA) and as well as how this should be addressed within the forthcoming Technical Rationale document. Please refer to the forthcoming CIP-005-7 Technical Rationale.
- **Commenters expressed concern with the overlap of CIP-012 and the "Super ESP."** The SDT thanks you for your comment. This potential overlap was resolved with the exclusion language proposed within CIP-005-7 R1.3.
- **Commenters expressed that "per system capability" should be added to the management plane isolation requirement.** The SDT thanks you for your comment. The SDT intends to address the "per system capability" scoping mechanism vs. requiring Technical Feasibility Exceptions where this is appropriate.
- **Commenters were concerned with the potential of continuing the EAP concept within the CIP standards and the potential of a one-to-one definition of EAP to Cyber Asset.** The SDT thanks you for your comment. The SDT has proposed retiring the EAP definition. With the move to an objective based requirement in CIP-005 and the need to not prescribe a cyber asset interface, an electronic access point, on a network boundary as the only model for addressing network access control, the term EAP is no longer used within the standard and is proposed to be retired. Entities are free to continue to use the term in their internal documentation to maintain backwards compatibility.
- **Commenters expressed that SCI needs to be better defined to highlight the differences between it and regular assets.** The SDT thanks you for your comment. The SDT has proposed the following definition for SCI: "Programmable electronic devices whose compute, storage (including network transport), or network resources are shared with one or more Virtual Cyber Assets or that perform logical isolation for an ESZ or ESP. This includes its management systems." The SDT's intent with this definition was to distinguish SCI from regular assets.
- **Commenters requested to address mixed use environments.** The SDT thanks you for your comments. The SDT intends to address the use of "mixed trust" through two methods. Please refer to the forthcoming Technical Rationale.

  The use of "affinity" within the Shared Common Infrastructure (SCI) will ensure that only Virtual Cyber Assets of the same "trust" level will be allowed to share CPU and system memory. This is to prevent the possibility that vulnerability within a Virtual Cyber Asset of lower trust level could be exploited to gain control of another Virtual Cyber Asset of higher trust level running on the same hypervisor within the SCI.

The high water marking of security requirements (i.e. “equalizing” or “high water marking” the R’s) results in some Virtual Cyber Assets now sharing equal trust levels. This allows these Virtual Cyber Assets to share the same CPU and system memory with the supporting SCI.

- **Commenters were concerned about the future consistent auditing approach of these modifications.** The SDT thanks you for your comment. The SDT has previously worked with NERC and the Regional Entity auditors on our approach and plan to continue working with the Monitoring and Enforcement teams as development of the standards progress.
- **Commenters expressed confusion over the options and the hypervisor isolation.** The SDT appreciates the support on the concepts of Virtual Cyber Assets, Virtual Storage and Remediation VLANs. In the Case for Change white paper, the SDT did not intend to imply that distributed firewalls, zero trust models and management plane isolation were not possible with the current standards. The intent was to show that because of how the current standards are written, using these technologies is not encouraged, and in fact could be discouraging these methods, with the amount of administrative overhead they could entail.

  The SDT has considered the comments on Management Plane Isolation and agrees. This is reflected in our proposed R1 for CIP-005.
- **Commenters expressed the desire to create two sets of standards (physical and virtual).** The SDT thanks you for your comment. The SDT asserts that the virtual vs physical assets perform the same function and it is difficult to ascertain which standard to apply to each asset as most entities use a hybrid configuration. The SDT is incorporating new definitions and objectives based requirements to address the differences between the two types. Requiring security objectives to be met should decrease the need to be prescriptive on the difference between physical and virtual systems.
- **Commenters expressed that the CIP standards already allow for virtualization.** The SDT thanks you for your comments. The SDT recognizes that some entities have already made use of Virtualization under the existing CIP Standards or contend that the existing CIP standards do not require any changes to accommodate Virtualization.

  The SDT contends that by moving the CIP standards forward from their existing “technical requirement” basis to a more “security objective” basis will result in better futureproofing as technology evolves.

  While many of the technical concepts utilized by virtualization currently exists and could be retrofitted within the existing CIP Standards, the move towards “policy based” security controls will better fit within the “security objective” based framework of CIP standards.
- **Commenters expressed a desire to include more compliance examples and clarity to better evaluate proposed changes.** The SDT intends to produce more detailed documentation in both the forthcoming Technical Rational and Implementation Guidance to assist entities to evaluate the proposed changes.

- **Commenters expressed the need to allow for backward compatibility.** The SDT thanks you for your comments. The SDT recognizes the substantial investment that entities have made in their programs to meet the existing CIP requirements. As such, the SDT has prioritized ensuring that backwards compatibility exists for current physical infrastructure installations.

  In some cases, full backwards is not possible as the SDT is also tasked with providing clarity in situations which were not envisioned in earlier versions of the CIP Standards. The forthcoming Technical Rationale document is intended to highlight where such situations exist.

- **Commenters expressed the need for clarity on “Super ESPs.”** The SDT thanks you for your comments. The SDT recognizes that entities need clarity on how situations involving how “Super ESPs” should be handled. Please refer to the forthcoming Technical Rationale document in the section entitled, “Requirement R1 Part 1.3”. The SDT contends that the new “Super ESP/ESZ” construct allows for cases where either routing cannot be used (such as layer 2 high speed database/ file replication) or where time sensitive data would be required to cross existing ESP boundaries (IEC-61850 GOOSE).

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Logical Isolation

2. **Number:** CIP-005-7

Purpose: To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication.

3. **Applicability:**

3.1. Functional Entities: For the purpose of the requirements in this standard, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. **Generator Operator**

4.1.4. **Generator Owner**

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

3.2. Facilities: For the purpose of the requirements in this standard, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

3.2.1.1 Each UFLS or UVLS System that:

3.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

3.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

3.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

3.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

3.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets, including third-party owned Cyber Assets, associated with communication networks and data communication links between discrete Electronic Security Perimeters or Electronic Security Zones.

4.2.3.3. Cyber Assets, including third-party owned Cyber Assets, associated with communication networks and data communication links used to extend a discrete ESP or ESZ to one or more geographic location.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

3.3. Effective Date: See Implementation Plan for Project 2016-02 (CIP-005-7).

4. **Background:** Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Logical Isolation. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Logical Isolation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	All applicable systems shall reside within one or more defined ESPs or ESZs.	An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Electronic Security Perimeters and Electronic Security Zones created in Part 1.1.	Require inbound and outbound logical access permissions, including the reason for granting access, and deny all other logical access by default. Excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	An example of evidence may include, but is not limited to, architectural diagrams that detail how network communication is limited and a list of rules (firewall, access control lists, software defined policies, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Security Zone or Electronic Security Perimeter that spans more than one geographic location containing: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems	Protect the confidentiality and integrity of the data traversing communication networks and data communication links used to extend an applicable ESP or ESZ, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	Evidence may include, but is not limited to, architecture documents detailing the methods used to mitigate the risk of unauthorized disclosure. Examples include physical protection and the points where encryption initiates and terminates.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	Perform authentication when establishing Dial-up Connectivity with applicable systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	Have one or more methods for detecting known or suspected malicious routable Internet Protocol (IP) communications to or from ESPs or ESZs.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	Shared Cyber Infrastructure that hosts High Impact BES Cyber Systems Shared Cyber Infrastructure that hosts Medium Impact BES Cyber Systems	Management systems may only share CPU, memory, or ESZ or ESP with other management systems and the management plane.	Examples of evidence may include, but is not limited to, documentation that includes the configuration of systems that enforce authentication and isolation such as: • Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS) • Physical isolated out-of-band network for dedicated management interfaces, embedded management interfaces • Compute configuration showing the isolation of the management plane resources (e.g., hypervisor, containers)

R2. Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-7 Table R2 –Remote Access Management* for all remote access that originates from outside of any of the entities' ESP's or ESZ's containing high or medium impact BES Cyber Systems or associated SCI. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA • SCI Medium Impact BES Cyber Systems with IRA and their associated: • PCA • SCI	Ensure that Interactive Remote Access is through an Intermediate System that is not inside an applicable ESP or ESZ.	Examples of evidence may include, but are not limited to, network, diagrams, or architecture documents.
2.2	Intermediate Systems associated with High Impact BES Cyber Systems. Intermediate Systems associated with Medium Impact BES Cyber Systems.	Protect the confidentiality and integrity of Interactive Remote Access between the client and the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	Intermediate Systems associated with High Impact BES Cyber Systems. Intermediate Systems associated with Medium Impact BES Cyber Systems.	Require multi-factor authentication to IS.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

2.4	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High Impact BES Cyber Systems and their associated:	Have one or more method(s) to disable active vendor remote access	Examples of evidence may include, but are not limited to, documentation

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	• PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	(including Interactive Remote Access and system-to-system remote access).	of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.
2.6	Intermediate Systems that are hosted on SCI and are associated with High Impact BES Cyber Systems. Intermediate Systems that are hosted on SCI and are associated with Medium Impact BES Cyber Systems.	IS may only share CPU, memory, or ESZ or ESP with other IS.	An example of evidence may include, but is not limited to, documentation that includes the following: configuration showing that the CPU and memory can only be shared with other IS.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The applicable systems shall keep data or evidence of Requirement R1 and Requirement R2 for 3 calendar years.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. Associated Documents

- CIP-005-7 Technical Rationale
- CIP-005-7 Implementation Guidance

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Logical Isolation ~~Electronic Security Perimeter(s)~~

2. **Number:** CIP-005-7~~6~~

Purpose: To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication. ~~To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.~~

3. **Applicability:**

3.1. Functional Entities: For the purpose of the requirements in this standard ~~contained herein~~, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and

including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

~~4.1.4.~~ Generator Owner

~~4.1.5.~~4.1.4. ~~Interchange Coordinator or Interchange Authority~~

~~4.1.6.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~4.1.7. Transmission Owner

3.2. Facilities: For the purpose of the requirements in this standard ~~contained herein~~, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

3.2.1.1 Each UFLS or UVLS System that:

3.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

3.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

3.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

3.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

3.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-6:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets, including third-party owned Cyber Assets, associated with communication networks and data communication links between discrete Electronic Security Perimeters or Electronic Security Zones.

~~4.2.3.2.~~4.2.3.3. Cyber Assets, including third-party owned Cyber Assets, associated with communication networks and data communication links used to extend a discrete ESP or ESZ to one or more geographic location.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

3.3. Effective Date: See Implementation Plan for Project 2016-02~~3~~ (CIP-005-7).

4. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.

- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- ~~**Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7~~6~~ Table R1 – Logical Isolation. ~~Electronic Security Perimeter.~~ [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-7~~6~~ Table R1 – Logical Isolation ~~Electronic Security Perimeter~~* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	All applicable systems ~~Cyber Assets connected to a network via a routable protocol~~ shall reside within one or more ~~a~~ defined ESPs or ESZs.	An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems. ~~Cyber Assets connected via a routable protocol within each ESP.~~

CIP-005-6 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
~~1.2~~	~~High Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~• PCA~~	~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~	~~An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.~~
1.2~~3~~	Electronic Security Perimeters and Electronic Security Zones created in Part 1.1. ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	Require inbound and outbound logical access permissions, including the reason for granting access, and deny all other logical access by default. Excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	An example of evidence may include, but is not limited to, architectural diagrams that detail how network communication is limited and a list of rules (firewall, access control lists, software defined policies, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.~~a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.~~

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Security Zone or Electronic Security Perimeter that spans more than one geographic location containing: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems	Protect the confidentiality and integrity of the data traversing communication networks and data communication links used to extend an applicable ESP or ESZ, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	Evidence may include, but is not limited to, architecture documents detailing the methods used to mitigate the risk of unauthorized disclosure. Examples include physical protection and the points where encryption initiates and terminates.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: - PCA - SCI - PACS hosted on SCI - EACS hosted on SCI Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: - PCA - SCI - PACS hosted on SCI - EACS hosted on SCI	~~Where technically feasible, p~~Perform authentication when establishing Dial-up Connectivity with applicable systems, per system capability. ~~Cyber Assets.~~	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: - PCA - SCI - PACS hosted on SCI - EACS hosted on SCI Medium Impact BES Cyber Systems at Control Centers and their associated: - PCA - SCI - PACS hosted on SCI - EACS hosted on SCI ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Cen~~	Have one or more methods for detecting known or suspected malicious routable Internet Protocol (IP) communications to or from ESPs or ESZs. ~~Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications~~	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	Shared Cyber Infrastructure that hosts High Impact BES Cyber Systems Shared Cyber Infrastructure that hosts Medium Impact BES Cyber Systems	Management systems may only share CPU, memory, or ESZ or ESP with other management systems and the management plane.	Examples of evidence may include, but is not limited to, documentation that includes the configuration of systems that enforce authentication and isolation such as: • Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS) • Physical isolated out-of-band network for dedicated management interfaces, embedded management interfaces • Compute configuration showing the isolation of the management plane resources (e.g., hypervisor, containers)

R2. Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, ~~where technically feasible,~~ in *CIP-005-7~~6~~ Table R2 –Remote Access Management* for all remote access that originates from outside of any of the entities' ESP's or ESZ's containing high or medium impact BES Cyber Systems or associated SCI. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-7~~6~~ Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: • PCA • SCI Medium Impact BES Cyber Systems with IRA ~~External Routable Connectivity~~ and their associated: • PCA • SCI	~~For all~~ Ensure that Interactive Remote Access is through an Intermediate System that is not inside an applicable ESP or ESZ. ~~, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~	Examples of evidence may include, but are not limited to, network, diagrams, or architecture documents.
2.2	Intermediate Systems associated with High Impact BES Cyber Systems.~~High Impact BES Cyber Systems and their associated:~~ ~~PCA~~	Protect the confidentiality and integrity of Interactive Remote Access between the client and the Intermediate System. ~~For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.~~	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~ Intermediate Systems associated with Medium Impact BES Cyber Systems.		
2.3	Intermediate Systems associated with High Impact BES Cyber Systems. Intermediate Systems associated with Medium Impact BES Cyber Systems. ~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~• PCA~~	Require multi-factor authentication to IS. ~~for all Interactive Remote Access sessions.~~	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

2.4	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems ~~with External Routable Connectivity~~ and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High Impact BES Cyber Systems and their associated:	Have one or more method(s) to disable active vendor remote access	Examples of evidence may include, but are not limited to, documentation

CIP-005-6 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
	• PCA • SCI • PACS hosted on SCI • EACS hosted on SCI • Medium Impact BES Cyber Systems ~~with External Routable Connectivity~~ and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	(including Interactive Remote Access and system-to-system remote access).	of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.
2.6	Intermediate Systems that are hosted on SCI and are associated with High Impact BES Cyber Systems. Intermediate Systems that are hosted on SCI and are associated with Medium Impact BES Cyber Systems.	IS may only share CPU, memory, or ESZ or ESP with other IS.	An example of evidence may include, but is not limited to, documentation that includes the following: configuration showing that the CPU and memory can only be shared with other IS.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- The ~~[~~applicable ~~entity(ies)]~~systems shall keep data or evidence of Requirement ~~X~~ R1 and Requirement R2 for ~~X~~3 calendar ~~days/months/~~years.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. Associated Documents~~None.~~

- CIP-005-7 Technical Rationale
- CIP-005-7 Implementation Guidance

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards

The Project 2016-02 Standard Drafting Team (SDT) is seeking comments on the following new, modified, or retired terms used in the proposed standard. Please note that Project 2016-02 is not proposing changes to Cyber Asset (CA), BES Cyber System (BCS), Electronic Security Perimeter (ESP), and External Routable Connectivity (ERC) definitions to maintain compatibility for non-virtualized systems.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset; excluding Shared Cyber Infrastructure, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Shared Cyber Infrastructure (SCI)		Programmable electronic devices whose compute, storage (including network transport), or network resources are shared with one or more Virtual Cyber Assets or that perform logical isolation for an ESZ or ESP. This includes its management systems.
Virtual Cyber Asset (VCA)		A logical instance of an operating system, firmware, or self-contained application hosted on Shared Cyber Infrastructure.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: - BES Cyber Asset, - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or - PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	A Cyber Asset or Virtual Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: - BES Cyber Asset, - Shared Cyber Infrastructure, - network within an Electronic Security Perimeter (ESP) or Electronic Security Zone containing high or medium impact BES Cyber Systems, or - PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.	Cyber Assets or Virtual Cyber Assets that control~~, alert, or log~~ access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Access Monitoring Systems (PAMS)		Cyber Assets or Virtual Cyber Assets that monitor, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	Cyber Assets or Virtual Cyber Assets that: • Are connected using a routable protocol within or on an Electronic Security Perimeter that are not part of the highest impact BES Cyber System within the same Electronic Security Perimeter; or • Are within the same Electronic Security Zone that are not part of the highest impact BES Cyber System within the same Electronic Security Zone; or • Share compute resources (CPU or memory) with a BES Cyber System.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	RETIRED
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	RETIRED
Electronic Access Control System (EACS)		Cyber Assets or Virtual Cyber Assets that provide electronic access control to an ESP, ESZ -or BES Cyber System.
Electronic Access Monitoring Systems (EAMS)		Cyber Assets or Virtual Cyber Assets that provide electronic access monitoring of an ESP, ESZ, or BES Cyber System.
Intermediate Systems (IS)	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	A type of EACS that is used to restrict Interactive Remote Access.
Electronic Security Zone (ESZ)		A segmented section of a network that contains systems and components to create logical isolation.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System from a Cyber Asset or Virtual Cyber Asset that is outside of its associated Electronic Security Perimeter or Electronic Security Zone via a bi-directional routable protocol connection.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated access by a person employing a remote access client.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border ~~surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for~~ at which access is controlled.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP or ESZ, ~~or~~ a Protected Cyber Asset, or SCI. ~~Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
CIP-005 and Associated Definitions

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on the **Virtualization Updates for CIP-005 and Associated Definitions** by **8 p.m. Eastern, Wednesday, September 11, 2019.**

Additional information is available on the project page. If you have questions, contact Standards Developer Jordan Mallory (via email) or at (404) 446-2589.

Background

Project 2016-02 addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and considers the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for Standard Drafting Team Consideration (V5TAG Transfer Document).

The V5TAG, which consisted of representatives from NERC, Regional Entities and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP Version 5 standards and to support industry's implementation activities. During the V5TAG's activities, it identified certain issues with the CIP Reliability Standards that would be better addressed by a standard drafting team (SDT) for the CIP Reliability Standards. The V5TAG developed CIP Version 5 Transition Advisory Group Issues for Consideration to document these issues. Among these issues, the V5TAG stated "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

The SDT proposed a path through an informal posting and comment period in November 2018 that did not receive acceptance via industry comments. Backwards compatibility, especially for environments unaffected by virtualization, must be a key component moving forward. The SDT drafted a "Case for Change White Paper" explaining why modifications to allow virtualization are needed and presented at a high level a more parallel approach to handling these issues. This approach used alternative definitions for the virtualized environments coupled with more objective requirements. The SDT received a large majority of positive comments on this approach. The current informal posting and comment period is the result of the work to date with this approach within CIP-005 and related definitions.

Also included in the posting are two other items:

- Proposed work on handling the V5TAG issue of ERC/IRA clarification in instances where a serial only device is converted to a routable protocol.
- Splitting the EACMS and PACS definitions such that the access control functions are separate from those systems that only monitor or log access and can be subject to differing requirements based on differing risk.

The standards that will be primarily impacted by these modifications will be CIP-005, CIP-007, and CIP-010 with conforming changes to many other CIP standards. This posting reflects only modifications to CIP-005 and associated definitions in order to get industry feedback as work begins on the other standards. The SDT is looking for feedback on the current approach of using Virtual Cyber Assets (VCA) and Shared Cyber Infrastructure (SCI) definitions to handle virtualized platforms and the new Electronic Security Zone (ESZ) concept that is a new proposed option in CIP-005 for scenarios that no longer fit the existing ESP/EAP model.

Summary of CIP-005 Changes

For a detailed explanation of these changes, please refer to the *CIP-005 Technical Rationale* document.

Questions

1. The SDT is proposing the new Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions to allow requirements to be specifically targeted at virtualized environments. The SDT is also proposing conforming changes in several other definitions to allow VCA's as an option. Do you agree with the development of new terms and the proposed definition of those terms? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (NOTE: Future CIP-011 requirements to be developed to address logical isolation within storage systems and will be coordinated with Project 2019-02 (BCSI)). (CIP-005 Technical Rationale pages 11-12).

   ☐ Yes

   ☐ No

   Comments:

2. The CIP SDT tried to maintain backwards compatibility throughout CIP-005. However, in order to take advantage of emergent technologies the existing firewall that were associated with an EAP will now fall into the SCI definition and be subject to CIP-005 Requirement R1 Part 1.6, which requires management plane separation. What level of effort would be required to accommodate these changes? Do you agree? If not, please provide comments to support your response. (CIP-005 Technical Rationale pages 11, 13, and 29-32).

   ☐ Yes

   ☐ No

   Comments:

3. The SDT is proposing the new term Electronic Security Zone (ESZ) to enable future technologies such as policy based environments. Do you agree with the proposed definition? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. Note: ESP will be retained for backwards compatibility. (CIP-005 Technical Rationale pages 10, 14-18, 22-26, and 38-40).

   - Electronic Security Zone (ESZ): A segmented section of a network that contains systems and components to create logical isolation.

   ☐ Yes

   ☐ No

   Comments:

4. The SDT is addressing the risk of systems of different impact, trust, or security levels (“mixed trust”) environments that are possible on Shared Cyber Infrastructure by modifying the definition of Protected Cyber Asset (PCA) so that it includes those VCA’s that can share a hypervisor’s CPU or memory. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 8, and 14-15).

   ☐ Yes

   ☐ No

   Comments:

5. The SDT proposes to address infrastructure that is shared between differing BCS impact ratings that share CPU and memory resources by aligning the CIP Requirements for all systems within an ESZ or ESP and affinity to prevent sharing of CPU and memory between Virtual Cyber Assets of differing impact ratings. Do you agree with these changes? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 11, 12, and 14).

   ☐ Yes

   ☐ No

   Comments:

6. The SDT is proposing the addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3 for “Super-ESP” scenarios where single ESP’s or ESZ’s span multiple geographic locations. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 18, and 25-26).

   ☐ Yes

   ☐ No

   Comments:

7. The SDT is proposing to retire EACMS and develop two new terms: EACS and EAMS. These terms will allow changes within the applicable systems column of the relevant requirements to allow third party monitoring. Monitoring and logging data will be handled within CIP-011 in a future posting. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. NOTE: Project 2016-02 will coordinate with Project 2019-02 (BCSI) and Project 2019-03 (Supply Chain) on this topic. (CIP-005 Technical Rationale pages 9, 10, 13, and 19).

   ☐ Yes

   ☐ No

   Comments:

8. The V5TAG document request the SDT to “Clarify the IRA definition to address the placement of the phrase “using a routable protocol” in the definition and clarity with respect to Dial-up Connectivity.” Therefore, the SDT proposes modifications to the IRA definition and CIP-005 Requirement R2. These modifications will clarify scenarios where Interactive Remote Access applies to serial only devices. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 7, 19-21, 27, and 33-37).

   ☐ Yes

   ☐ No

   Comments:

9. The SDT is proposing modifications to CIP-005 Requirement R1. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rational pages 22-32).

   ☐ Yes

   ☐ No

   Comments:

10. The SDT is proposing modifications to CIP-005 Requirement R2. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rationale pages 33-37).

    ☐ Yes

    ☐ No
    Comments:

11. Backwards Compatibility: What level of effort is required to migrate from existing definitions to new definitions on existing virtualized architecture?

    Comments:

12. The SDT posted a draft CIP-005-7 Technical Rationale document to explain the basis behind these proposed changes. Please provide any additional comments on this document.

    Comments:

13. Provide any additional comments for the SDT to consider, if desired.

    Comments:

DRAFT

Cyber Security – BES Cyber System Logical Isolation

Technical Rationale and Justification for Reliability Standard CIP-005-7

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

This document is the technical rationale and justification for the proposed Reliability Standard CIP-005-7. The Standard Drafting Team's (SDT) intent of this document is to provide stakeholders and the ERO Enterprise with an understanding of the proposed revisions and the technical concepts of the Reliability Standard. This Technical Rationale and Justification for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Executive Summary

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. The Standard Drafting Team (SDT) is proposing changes to CIP-005-6 as it updates the standards based on technology innovation and changes such as the increasing use of virtualization. Project 2016-02 SDT was assigned the task to address the technological innovation in virtualization within the CIP standards. The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards. The SDT's intent is to better position the CIP standards to be applicable to additional future technological innovation.

The Project 2016-02 CIP SDT proposes the following modified terms within the NERC Glossary:

- BES Cyber Asset (BCA);
- External Routable Connectivity (ERC);
- Interactive Remote Access (IRA);
- Intermediate System (IS);
- Physical Access Control System (PACS);
- Physical Security Perimeter (PSP);
- Protected Cyber Asset (PCA);
- Removable Media (RM); and
- Transient Cyber Asset (TCA).

The Project 2016-02 CIP SDT proposes the following new terms to the NERC Glossary:

- Electronic Access Control Systems (EACS);
- Electronic Access Monitoring System (EAMS);
- Electronic Security Zone (ESZ);
- Physical Access Monitoring System (PAMS);
- Shared Cyber Infrastructure (SCI); and
- Virtual Cyber Asset (VCA).

The Project 2016-02 CIP SDT proposes to retire the following terms:

- Electronic Access Control and Monitoring System (EACMS); and
- Electronic Access Point (EAP).

These modified terms, new terms, and retired terms are further explained herein.

The title and purpose of CIP-005-7 changed from Electronic Security Perimeters to Logical Isolation. ESP's and EAPs remain a valid option and are one method for implementing logical isolation. However, virtualized technologies present other equally effective methods than ESPs that deal only with layer 3 routable protocol addressing. To adapt virtualization's characteristics, CIP-005-7 focuses on logical isolation such that high and medium impact BES Cyber Systems be "logically isolated" from all other systems (regardless of protocol) to replace the routable protocol-based ESP requirement as the solitary method that may be used.

Another concept introduced within CIP-005-7 is shared infrastructure. For virtualized environments where shared infrastructure (hardware) is used, a risk of side channel attacks exists. CIP-005-7 proposes to require the placing of virtualized systems of differing trust levels into differing ESZ's, and then affinity controls must be applied to these zones. These affinity groups must be configured such that a hypervisor does not allow workloads in these differing zones to simultaneously exist or execute on the same hardware underlay compute resources.

Additionally, the SDT is proposing a new requirement (CIP-005-7 R1.6) to separate the management plane of the SCI from the data plane. This is needed to ensure the reliability and security of the management plane.

CIP-005-7 also introduces exemptions and requirements for extending ESPs or ESZs across geographic locations also known as "Super ESPs". This allows, for example, entities to extend a network to replicate data at high speed between two virtualization infrastructures (SCI) or two databases in two different geographic locations to improve the resilience and reliability of BES Cyber Systems. Requirement 1 Part 1.3 within CIP-005-7 requires that data traversing "Super ESPs" be protected to preserve its integrity and confidentiality.

Proposed Modified Terms:

BES Cyber Asset (BCA)

A Cyber Asset or Virtual Cyber Asset; excluding Shared Cyber Infrastructure, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Rationale

The BCA definition is changing to allow for BES Cyber Assets to be either Cyber Assets (hardware included) or Virtual Cyber Assets (without the underlying hardware). The definition of BCA excludes the underlying hardware for virtualized environments, now defined as Shared Cyber Infrastructure (SCI). The SDT recognizes that SCI indeed has the same impact as a virtual BES Cyber Asset and even more so if hosting numerous BES Cyber Assets. For the first formal posting of all affected standards, the requirements for SCI will be equal to BCA and in fact be subjected to additional requirements due to its impact (e.g. CIP-005 R1 Part 1.6). See the SCI definition below.

External Routable Connectivity (ERC)

The ability to access a BES Cyber System from a Cyber Asset or Virtual Cyber Asset that is outside of its associated Electronic Security Perimeter or Electronic Security Zone via a bi-directional routable protocol connection.

Rationale

The ERC definition is used throughout the CIP Standards, within the Applicable Systems column, as a scoping mechanism based on the inherent risk associated with external routable connectivity. In order to maintain the correct ERC scoping the SDT made conforming changes to the ERC definition to include both Virtual Cyber Assets and ESZs, but maintained the caveat of “via a routable protocol connection.” This effectively updates the ERC term to include the applicable new concepts presented within the updated CIP Standards.

Interactive Remote Access (IRA)

User-initiated access by a person employing a remote access client.

Rationale

The IRA definition is changing to remove several requirements and scoping mechanisms that were embedded within it so that it becomes a simple glossary definition. The requirements and scoping mechanisms have been moved into CIP-005 R2. The references to ownership of the remote client have been removed as immaterial to the definition or the CIP-005 requirements. The reliance on “using a routable protocol” has been removed to incorporate IP to serial conversion scenarios to serial only Cyber Assets. See discussion under the General Considerations section below.

Intermediate Systems (IS)

A type of EACS that is used to restrict Interactive Remote Access.

Rationale

The IS definition is changing to remove requirements-like language (e.g. where an IS must reside) that was embedded within the definition. Such language has been moved to CIP-005 R2.

Physical Access Control Systems (PACS)

Cyber Assets or Virtual Cyber Assets that control access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Rationale

The PACS definition is changing to 1) allow Virtual Cyber Assets as a form that PACS can take, and 2) separate out the non-access control functions (see PAMS below). This will allow differentiation in requirements based on the different risk profiles of a system that controls physical access versus systems that only log or alert (i.e. a SIEM or internal or outsourced monitoring service). The intent is that a system that both controls and monitors physical access remains a PACS. If the system controls physical access, it is a PACS regardless of its monitoring capabilities.

Physical Security Perimeter (PSP)

The physical border at which access is controlled.

Rationale

The PSP definition is changing to remove references to EACMS and other applicable systems. The applicability of the CIP-006 PSP requirements was included within the definition, so as the applicability of the requirements change over time (such as adding SCI), the definition would need to change. The SDT is proposing to remove not only the proposed retired term EACMS but all applicability from the definition to avoid current and future issues.

Protected Cyber Asset (PCA)

Cyber Assets or Virtual Cyber Assets that:

- Are connected using a routable protocol within or on an Electronic Security Perimeter that are not part of the highest impact BES Cyber System within the same Electronic Security Perimeter; or
- Are within the same Electronic Security Zone that are not part of the highest impact BES Cyber System within the same Electronic Security Zone; or
- Share compute resources (CPU or memory) with a BES Cyber System.

Rationale

The PCA definition is being updated to include the ESZ option so that Cyber Assets within an ESZ that are not part of the highest impact BES Cyber System within the zone become an associated PCA of the highest impact BES Cyber System.

The definition is also being updated to include “share compute resources (CPU or memory) with a BES Cyber System” to mitigate the risks of hardware-based vulnerabilities (Spectre, Meltdown, Rowhammer, etc.) on Shared Cyber Infrastructure. Since virtualization can allow systems of differing trust levels to simultaneously execute on the same hypervisor servers in the hardware underlay and thus share the same CPU and memory, this addition to the PCA definition requires that those VCAs that do share CPU and memory become associated PCA’s of any BES Cyber Systems sharing the same hypervisor compute resources. This provides the high water marking of VCAs sharing a single hypervisor’s CPU or memory.

See the “Shared Infrastructure and ‘Mixed Trust’ Risks” section below for a more in-depth discussion.

Removable Media

Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP or ESZ, a Protected Cyber Asset, or SCI.

Rationale

The Removable Media definition has conforming changes to allow the targets to which the media may be connected include SCI and a network within an ESZ.

Transient Cyber Asset (TCA)

A Cyber Asset or Virtual Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
    - BES Cyber Asset,
    - Shared Cyber Infrastructure (SCI),
    - network within an Electronic Security Perimeter (ESP) or Electronic Security Zone (ESZ) containing high or medium impact BES Cyber Systems, or
    - PCA associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Rationale

The TCA definition is changing to incorporate the virtualization definitions in three ways. First, VCA is being added as a form a TCA can take. The intent is to handle VCAs that are created for typical TCA uses but are normally dormant (e.g. a Virtual Machine (VM) with Wireshark for troubleshooting network issues within a virtualized infrastructure). Secondly, SCI was added as a target to which TCA's can be directly connected. Thirdly, conforming changes were made to add connection to a network within an ESZ as an option.

Proposed New Terms:

Electronic Access Control Systems (EACS)

Cyber Assets or Virtual Cyber Assets that provide electronic access control to an ESP, ESZ, or BES Cyber Systems.

Rationale

The EACMS definition is splitting into two terms. The EACS definition is proposed to 1) allow Virtual Cyber Assets as a form that EACS can take, and 2) separate out the non-access control functions. This will allow differentiation in requirements based on the different risk profiles of a system that controls access (i.e. a firewall) versus systems that only log or alert (i.e. a SIEM or internal or outsourced monitoring service). The intent is that a system that both controls and monitors electronic access remains an EACS. If the system controls electronic access, it is an EACS regardless of its monitoring capabilities.

Electronic Access Monitoring System (EAMS)

Cyber Assets or Virtual Cyber Assets that provide electronic access monitoring of an ESP, ESZ, or BES Cyber Systems.

Rationale

The EACMS definition is splitting into two terms. The EAMS definition is proposed to 1) allow Virtual Cyber Assets as a form that EAMS can take, 2) incorporate ESZs, and 3) separate out the non-access control functions. This will allow differentiation in requirements based on the different risk profiles of a system that controls access (i.e. a firewall) versus systems that only log or alert (i.e. a SIEM or internal or outsourced monitoring service).

Electronic Security Zone (ESZ)

A segmented section of a network that contains systems and components to create logical isolation.

Rationale

In previous versions of the CIP standards, CIP-005 required declarations of Electronic Security Perimeters (ESP) based on OSI layer 3 routable protocols. All BES Cyber Assets (BCA) that were connected to a network with routable protocols had to reside inside a declared ESP. Any External Routable Connectivity (ERC) to the BES Cyber Systems inside the ESP had to enter and exit via an Electronic Access Point (EAP) that limited the traffic entering or leaving the ESP to only necessary traffic. It denied all other traffic by default.

This “castle and moat with drawbridge” protection, where the castle is the BES Cyber Systems (BCS), the moat is the ESP, and the drawbridge is the EAP, has been in place for many years. For many situations, the ESP/EAP model remains a valid network architecture however it is no longer the only model. Prescribing the ESP/EAP as the sole model hinders the adoption of other models that are equally or even more effective. Network access control is expanding beyond perimeter-based security at routable protocol address levels into other models where access controls are enforced within the network fabric itself. The entire network is becoming “the firewall” rather than a centralized point at a network boundary. Within virtualized environments, entities can describe network access at a policy level within a *zone* and zones may not follow the typical IP subnet defined network space. Zones allow for network access permissions to be applied to workloads based on their function and/or trust level rather than purely by network location which for resiliency purposes can be very dynamic. If a virtual machine is a member of a zone, it gets that zone’s access permissions applied to it regardless of its network location. IP addresses and port numbers, which are simply protocol data, become less common methods of identifying and filtering communications, especially in virtual environments where workloads dynamically move and may change network location but stay within the same zone. The zone’s policies follow the workload, not a network address range. This is driving solutions more towards policy-based user access controls for workloads that the infrastructure then dynamically applies within the environment.

In essence, as network access controls become embedded into the infrastructure, these environments may no longer have an “Electronic Access *POINT*”; no single interface on a perimeter where network access rules are enforced but are instead highly distributed within the network. This is the reason the CIP standards are adding the ”Electronic Security Zone” (ESZ) concept as an option that can be chosen for systems in addition to or in place of the ESP/EAP model.

Physical Access Monitoring System (PAMS)

Cyber Assets or Virtual Cyber Assets that alert or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Rationale

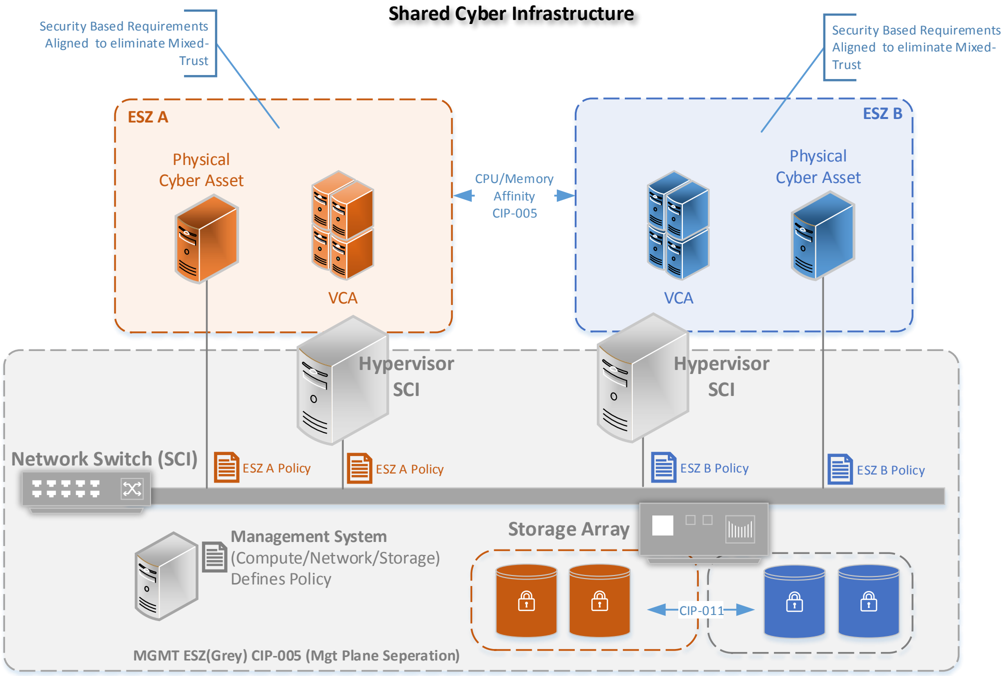
The PACS definition is splitting into two terms. The PAMS definition is proposed to 1) allow Virtual Cyber Assets as a form that PAMS can take, and 2) separate out the non-access control functions. This will allow differentiation in requirements based on the different risk profiles of a system that controls access (i.e. a badging system) versus systems that only log or alert (i.e. a SIEM or internal or outsourced monitoring service that only receives data).

Shared Cyber Infrastructure (SCI)

Programmable electronic devices whose compute, storage (including network transport), or network resources are shared with one or more Virtual Cyber Assets or that perform logical isolation for an ESZ or ESP. This includes its management systems.

Rationale

The SCI definition is being created to separate the underlying hardware from the VCAs that it hosts. This allows security requirements to be targeted to SCI to address the unique risks of virtualization and shared hardware. There are many requirements that now include the newly defined term SCI in the “Applicable Systems” column to maintain security level parity with traditional Cyber Assets. This change is justified because the hardware underlay would not have required protections at the same level as an applicable virtual system without this inclusion.



Beyond security level parity with protecting a typical hardware based Cyber Asset, the SCI can have a more significant impact in a virtualized environment since it can host, and therefore impact, multiple virtualized systems. Because of this capability, some additional controls only apply to SCI, such as the management plane isolation required by the proposed CIP-005-6 R1.6.

The statement “or performs logical isolation for an ESZ or ESP” is found within the Shared Cyber Infrastructure definition. This inclusion is intended to ensure that devices that provide logical isolation for an ESZ or ESP, and therefore have an associated risk, have protection for the associated management systems (management plane) as required by Part 1.6. This inclusion is meant to ensure protection of firewalls or network switches if used to provide logical isolation to an ESP, ESZ, or within Shared Cyber Infrastructure (see discussion and examples under the R1.6 section below). This can be viewed as a replacement for the Electronic Access Point (EAP) found in the previous version of the standard.

In the diagram above, an orange ESZ and a blue ESZ are depicted. Each ESZ contains VCAs and a physical Cyber Asset along with storage configured within a storage array. The individual ESZs are defined via policies created in the management system that are implemented by the SCI to create the logical isolation of that zone within the SCI’s compute, network, and storage resources. The SCI for this scenario is depicted in grey and includes the hypervisor servers, the network switch, the storage array hardware, and the management system(s) for each.

Virtual Cyber Asset (VCA)

A logical instance of an operating system, firmware, or self-contained application hosted on SCI.

Rationale

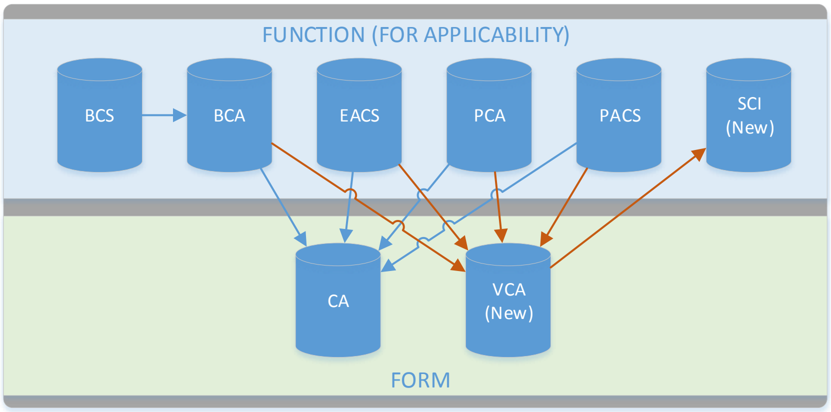
The NERC Glossary definition of Cyber Asset has a direct tie to the hardware on which it relied. This affected the definitions of the “Applicable Systems” terms such as BES Cyber Systems (BCS), EACS, PACS, and Protected Cyber Assets (PCAs). Because the Reliability Standard is applicable to the aforementioned systems, the control for the Cyber Assets also applies to the hardware. This tie to hardware implies a singular one BCA, EACS, PACS or PCA per individual hardware system. This one-to-one relationship between a Virtual Cyber Asset and its underlying hardware is what virtualization intentionally breaks to increase reliability and resiliency by allowing Virtual Cyber Assets to be abstracted from a particular hardware cyber asset and therefore able move to any available hardware out of a pool of resources.

The proposed NERC Glossary definition of Virtual Cyber Asset (VCA) allows the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined. The definition of VCA is not inclusive of hardware, and the EACS, PACS and PCA definitions have been updated to allow for VCA versions. With the addition of SCI and revisions to the “Applicable Systems”, there can be one or more virtualized instances of a BCA, EACS, PACS or PCA that reside on SCI.

Examples of Virtual Cyber Assets may include, but are not limited to, logical instances of the following:

- Operating Systems (Virtual Machines (VM));
- Containers, which are executable software package images that are standalone and self-contained;
- Networking devices such as switches, routers, and load balancers;
- Security appliances such as firewalls and VPN concentrators; and
- Helper appliances with logical connectivity (such as malware detection, plugins, etc.).

This diagram depicts the relationship between many of the glossary definitions in that some are the “form” of an object and some are the “function” it provides. The top row shows definitions of “functions” or services that are performed or provided. The bottom row is the “form”. Previously the only form that existed was the Cyber Asset definition which included the hardware and historically had a 1:1 relationship (e.g. a digital relay, a desktop computer operator workstation, a database server in a rack, etc.). The addition of the Virtual Cyber Asset definition clarifies a new form that the functions can take which is abstracted from the underlying hardware. The new SCI definition provides the functions of compute, network, and storage resources and logical isolation for VCAs. The blue arrows are the existing definitional relationships and the red arrows are the new definitional relationships that are being added.



Proposed Retired Terms:

EACMS

Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

Rationale

The EACMS definition is splitting into two terms (EACS and EAMS) to allow differentiation in requirements based on the different risk profiles of a system that controls access (i.e. a firewall) versus systems that only log or alert (i.e. a SIEM or internal or outsourced monitoring service). The combined term is proposed to be retired.

EAP

A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Rationale

With the move to an objective based requirement in CIP-005 and the need to not prescribe a cyber asset interface, an electronic access POINT, on a network boundary as the only model for addressing network access control, the term EAP is no longer used within the standard and is proposed to be retired. Entities are free to continue to use the term in their internal documentation to maintain backwards compatibility. See also the discussion for the SCI and ESZ definitions.

Logical Isolation

The title and purpose of CIP-005-7 changed from Electronic Security Perimeters to Logical Isolation. ESP's and EAPs remain a valid option and are one method for implementing logical isolation. However, virtualization technologies present other equally effective methods than ESPs that deal only with layer 3 routable protocol addressing. Virtualization and its accompanying shared infrastructure have other characteristics such as shared computing hosts, shared storage, shared virtual networks and switches, all of which pose different security concerns but also have different security controls. To adapt to these changes, CIP-005-7 focuses on an objective-based requirement (in Requirement Part 1.2) for logical isolation.

The SDT chose the term "logical isolation" to distinguish the type of isolation required from complete isolation or physical isolation alone. Logical isolation refers to the isolation of communications between systems. Two BES Cyber Systems can be physically isolated into two different access-controlled areas, but still have uncontrolled communication between them. Also, two virtual cyber systems within two different ESZs or ESPs of differing trust or impact levels may be running on two hypervisors within the same physical area, but still be logically isolated from each other. *Logical isolation means that only known, controlled communications can occur between a system and anything outside of its ESZ or ESP and that all other communication is blocked.* Serial communications such as RS-232 or RS-485 are logically isolated communications methods as well. These types of communications move data from the TX pin on one end of a cable to the RX pin on the other end of the cable. There is no addressing scheme or routing/firewall capability, so it meets the intent of logical isolation.

If a BCS is executing on a virtual host along with another related virtual machine that may not have a 15-minute impact, (e.g. a control system and its data historian), the entity must either consider all these workloads as part of a single system or declare the system with the 15-minute impact as a BCS and the historian as a separate system. If the latter is chosen, the entity will need to prove that the two systems are logically isolated and that every communication between the two is limited to only what is necessary.

Logical isolation is also relevant to other layers of a computing stack. Imagine in a virtualized data center where you are looking at a BES Cyber System architecture "from the side". You can see the different layers of the system, from the storage on a Storage Area Network (SAN) through the virtual networks, switches, and firewalls at the virtual network layer, up to the virtual hosts that are executing the application workloads. If you rotate the view until you are looking down at the system from above, you should be able to see the touch points of all these layers to other systems. Logical isolation refers to this top-down view. An entity needs to be able to show that only necessary data flows are allowed through any of these layers that have an interface to another system. For example, at a storage layer, BCS systems should have their storage logically isolated from other systems that are not part of the BCS. At a networking layer, there should be no communications channels that allow the BCS to talk to any other system that is not controlled. At a virtual machine level, there should be logical isolation between VMs. As you "look down" through the computing stack, you should only see interface points that are controlled and locked down to a least-privilege position. To allow for implementation of this isolation, the ESZ concept has been introduced so that systems of the same trust level can be placed into their own ESZ and the controls placed on the zone.

Shared infrastructure and "Mixed Trust" Risks

For virtualized environments where shared infrastructure (hardware) is used, a risk of side channel attacks exists. Virtualization allows disparate workloads of what could be differing impact or trust levels to execute on the same CPUs and share the same RAM within the infrastructure. There are vulnerabilities that are directly related to sharing hardware such as Spectre, Meltdown, and Rowhammer. Rowhammer for example concerns processes sharing certain forms of hardware memory such as DRAM. Repeated writing of bits in one process could flip bits in a process in adjacent physical memory. This type of vulnerability is one of the unique risks of Shared Cyber Infrastructure.

As this class of vulnerability is specifically about processes executing side by side on the same CPU or memory chips in a SCI environment, the risk of these vulnerabilities is being mitigated in CIP-005-7 by either:

- Declaring the VCAs that share compute resources (CPU, memory) or are within the same ESZ or ESP with a BES Cyber System as associated PCAs which will require they meet the same security requirements (high water marking); or
- Configuring the virtualization infrastructure to place VCA's of differing impact or trust levels into differing ESZ's and configuring affinity controls to these zones such that hypervisors do not allow workloads in these differing zones to simultaneously exist or execute on the same hypervisor.

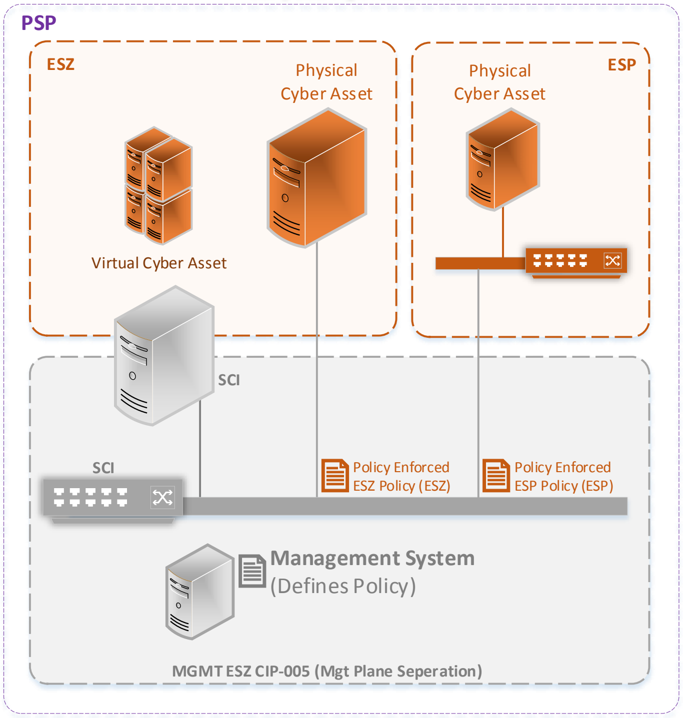
Hybrid Virtual/Physical Scenarios with ESP/ESZ's

Typically, virtualized environments will use the ESZ structure and physical asset environments will use the ESP structure for meeting CIP-005 requirements. However, numerous scenarios will include a hybrid of both virtual and physical Cyber Assets. An entity could configure their SCI so that both virtual and physical Cyber Assets are in the same ESZ to reduce the number of zones required to implement the new concepts. The following series of diagrams illustrates some hybrid scenarios.

Hybrid ESP/ESZ Inside of a Single PSP

In this scenario, a virtual Cyber Asset and physical Cyber Asset are shown with logical isolation (ESZ) provided by SCI using a policy enforced ESZ. Another physical Cyber Asset is show using an ESP for logical isolation. In this case, the same SCI is used to provide both the equivalent EAP functionality and logical isolation (ESP) via a policy enforced ESZ. Note that the management plane of the SCI resides within its own ESZ.

ESP/ESZ Hybrid Model



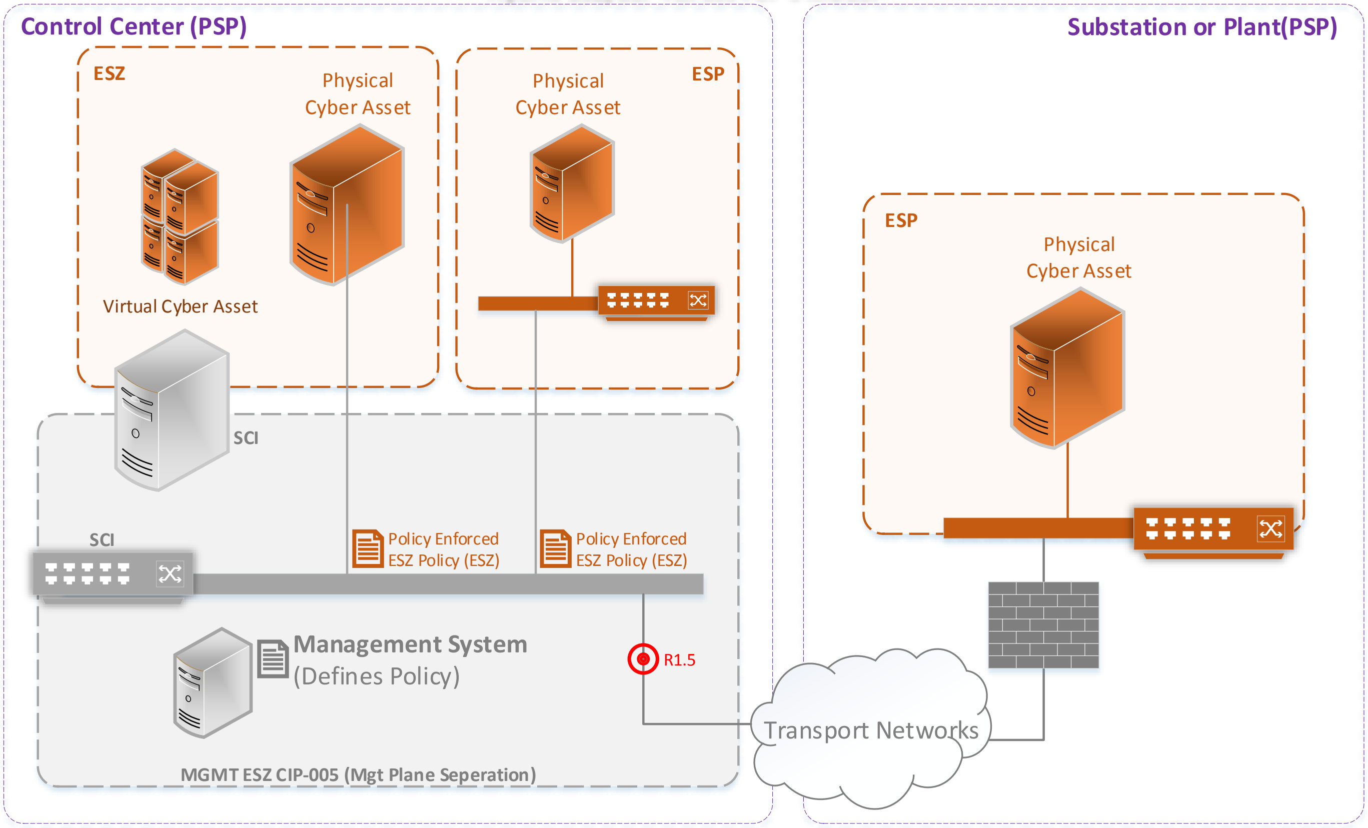
Hybrid ESP/ESZ across PSP's

In the left portion of this scenario (the Control Center), a virtual Cyber Asset and physical Cyber Asset are shown with logical isolation provided by SCI using a policy enforced ESZ. Another physical Cyber Asset is shown using an ESP for logical isolation. In this case, the same SCI is used to provide both the equivalent EAP functionality and logical isolation (ESP) via a policy enforced ESZ. Note that the malicious communications detection required for the Control Center (R1.5) is being provided by the SCI.

In the right portion of the drawing (Substation or Plant), another physical Cyber Asset is shown where its logical isolation is provided by an ESP. A physical firewall (EACS/SCI) is used to provide the logical isolation.

Note that the management plane of the SCI resides within its own ESZ.

Hybrid ESZ/ESP Across PSP's Model



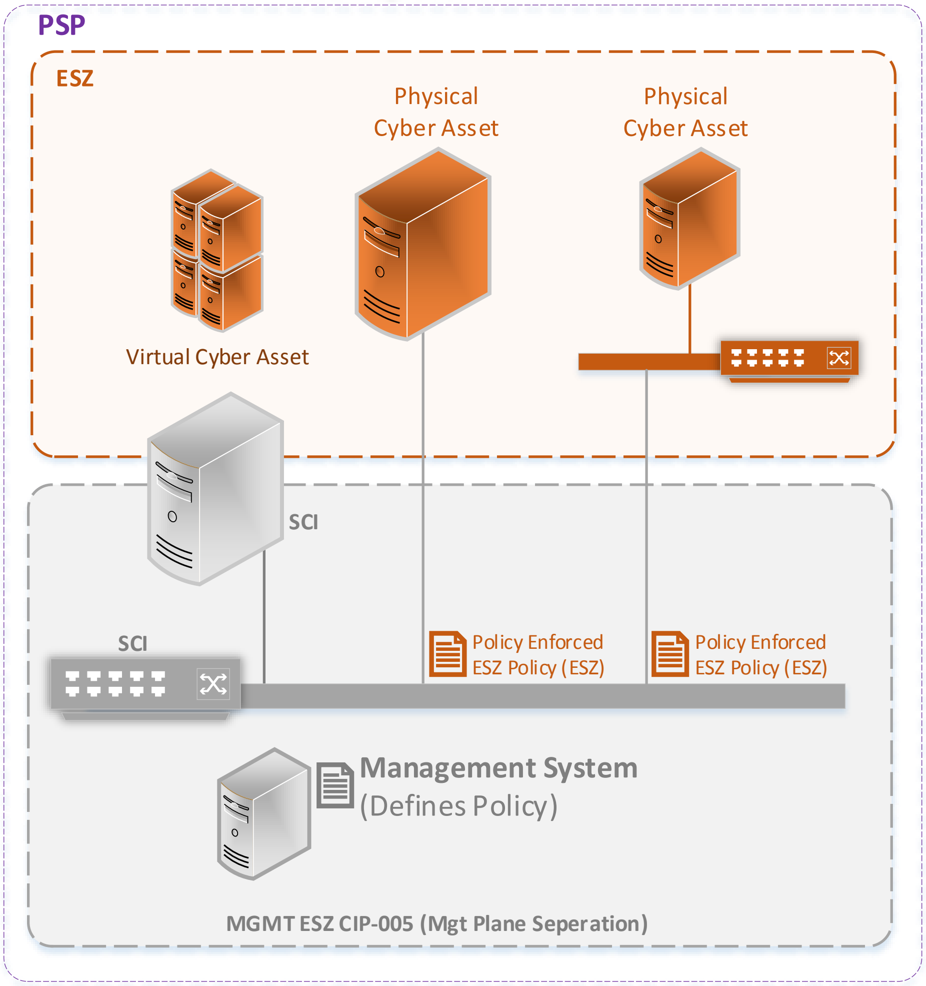
Combined ESZ for Cyber Assets and Virtual Cyber Assets

In this drawing, virtual and physical Cyber Assets are located within a single ESZ where the logical isolation is provided by the SCI. Previously, this would have required a physical firewall to both provide an EAP and logical isolation. In the left portion of the drawing, a VCA and supporting SCI are being utilized where logical isolation (ESZ) is being provided by the SCI using a policy enforced ESZ. The SCI is also enforcing logical isolation for the physical Cyber Assets by configuring the appropriate policy enforced ESZ. This effectively converts what would have been an ESP for the physical Cyber Assets into a similar policy enforced ESZ used by the virtual Cyber Asset where traditional EAP functionality is now provided by the SCI. This has the following advantages:

a) Access control for this environment is centrally managed and a single policy for the ESZ is enforced for virtual and physical Cyber Assets.

b) For applicable Control Centers, it alleviates the need for a multiple ESPs or ESZs and methods to detect malicious communication for network traffic between them within the Control Center.

Note that the management plane of the SCI resides within its own ESZ.

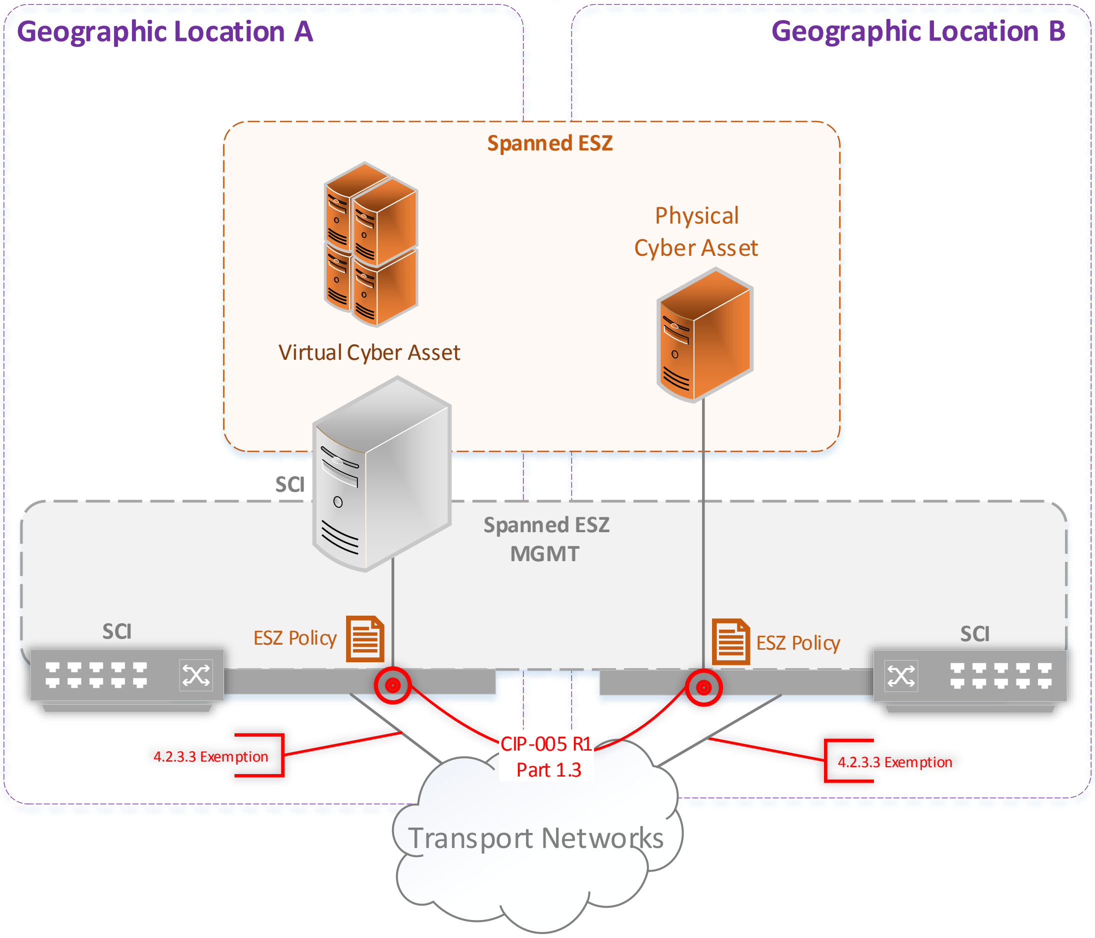


ESZ Replaces ESP Model

Spanned ESZ Model

In this model, two different geographic locations are connected by a transport network. The transport network is utilized to span the SCI and the same logical isolation (a single ESZ) between these two locations. In one location, a virtual Cyber Asset running on SCI is within the policy enforced ESZ. In the other location, a physical Cyber Asset is within the same ESZ that is spanned between the two locations. This allows the exact same ESZ policy to be enforced across the locations as well. Note that malicious communication detection is not required for network traffic within the same ESZ, even if it flows between the locations. However, the network data traversing the transport network must still be protected under CIP-005-7 Requirement R1.3 or CIP-012-1 where applicable.

Note that as the same management plane of the SCI is spanned between locations, the ESZ protecting the SCI management plane is also spanned as well.



Super (Spanned) ESZ/ESP Model

EACMS/PACS Glossary Terms

As technologies and attacks have advanced and become more complex, entities are becoming more interested in partnering with outside and government security services. These includes services like NERC's Cyber Security Risk Information Sharing Program (CRISP), Cybersecurity for the Operational Technology (OT) Environment (CYOTE), and those of other external security services and internal monitoring centers. Going forward, these types of service and providers will become more cloud based. Security service providers have visibility into emerging threats and trends that come through their extensive collections of information. Analysis of this information can then be shared more broadly, improving the overall cybersecurity posture and reliability of the BES through early detection of compromise and the ability to monitor for threats and indicators of compromise (IOCs) at machine speeds.

Under the current body of CIP Standards, using the types of services that include electronic access monitoring data (not involved in the actual control of electronic access) may bring all Cyber Assets involved into scope as an EACMS. This may discourage or even preclude entities from using these services based on the Cyber Asset level requirements of an EACMS. These limitations affect personnel, physical security, patching, baselines, and other requirements that focus on a Cyber Asset. Entities may also be discouraged from providing and correlating security events across enterprise and control networks, even though most cyber-attacks against control systems today enter through business networks. There is great value in correlating security events seen across enterprise and OT networks that may be discouraged or precluded through the "M" in EACMS growing to include much an enterprise's other monitoring only Cyber Assets.

The cyber systems that do perform electronic access control will remain as they are today in the standards. Those cyber systems, such as firewalls and routers with ACLs and other systems that do perform access control and actively protect the networks to which BES Cyber Systems are connected should not change. However, the monitoring and logging aspect of EACMS presents a different risk of information protection. The creation of two different defined terms recognizes this. EACS represents those systems that do control electronic access and will essentially be a drop-in replacement for today's EACMS.

The parallel also exists for PACS where a differentiation between systems that control physical access can be made with systems that only monitor or log access information.

External Routable Connectivity (ERC) and Interactive Remote Access (IRA)

External Routable Connectivity (ERC) is used in the CIP standards for different purposes, including:

1. Establishing when EAPs are required
2. Limiting scope of ~38 requirement parts to those locations that have a high enough level of remote connectivity to support the requirement

The move to the more objective-based requirements shifts the obligation away from implementing access controls at a defined cyber asset interface point (EAP). The objective can now be accomplished without dictating any architecture or access control method, thus eliminating ERC's role in determining EAPs. However, ERC is still needed as a scoping mechanism for the vast scale of systems and their components within a geographically distributed BES. Many requirement parts should be scoped based on whether the system has ERC for the following reasons:

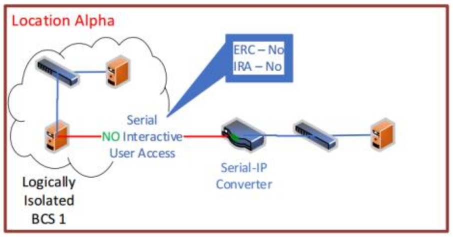
- The risk is increased for systems with ERC. The requirement should apply to those systems with an increased attack surface and risk due to their connectivity/accessibility.
- Locations that have legacy connectivity such as non-routable serial leased circuits should not have to increase their level of remote connectivity and attack surface to meet security requirements. For example, it would

not be advisable to put in an IP network into a site to get SNMP traps out for alerts if a serial circuit with reduced attack surface is all that is needed for operations.

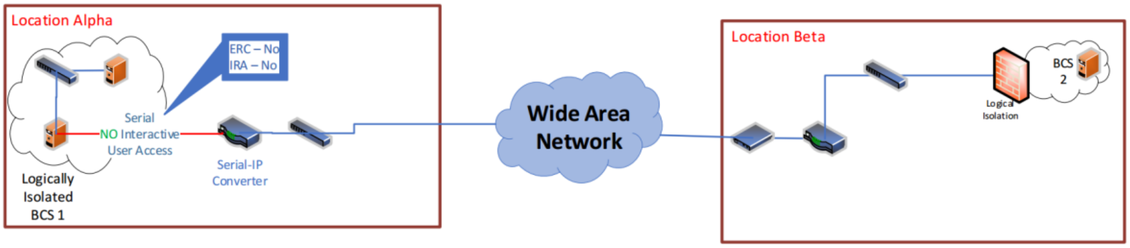
One issue with the ERC definition from the V5TAG transfer document has been that of BES Cyber Assets (BCA) that only speak non-routable protocols over a serial port. These BCAs are not in an ESP and therefore can be considered to not have ERC because it is defined in terms of an "associated ESP." These BCAs, however, can have Interactive Remote Access through an upstream serial-to-IP conversion. The SDT has kept ERC as-is with only conforming changes in order to not disrupt its scoping function as noted above. However, the IRA definition has been modified so that a device with only a serial, non-routable connection can now have IRA and be subject to CIP-005 R2. Appropriate controls (CIP-005 R2) are now required for these Interactive Remote Access sessions without regard to ERC.

The following diagrams show different scenarios and whether ERC and/or IRA exist in the situation.

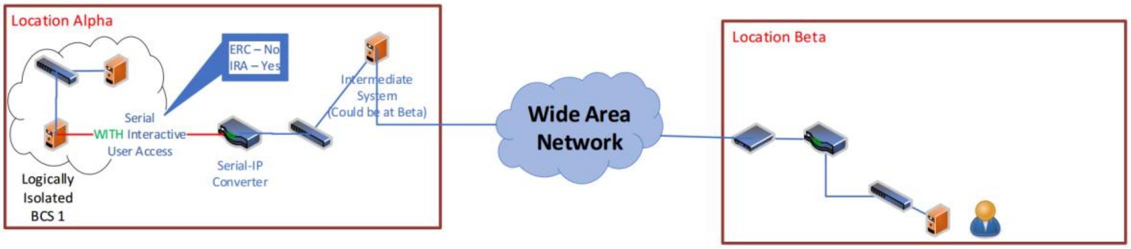
Local Serial Data



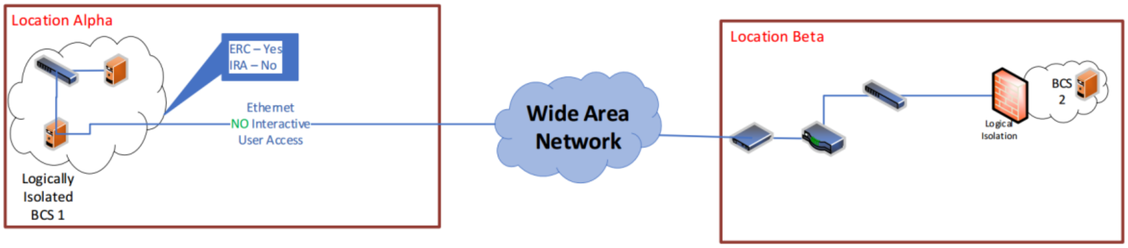
Remote Serial Data w/IP Conv



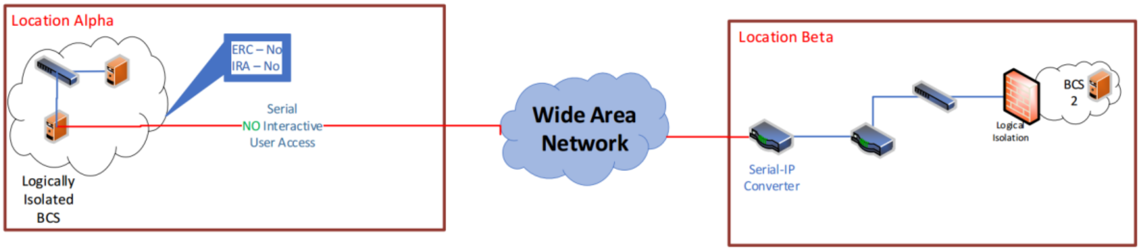
Remote Serial Access



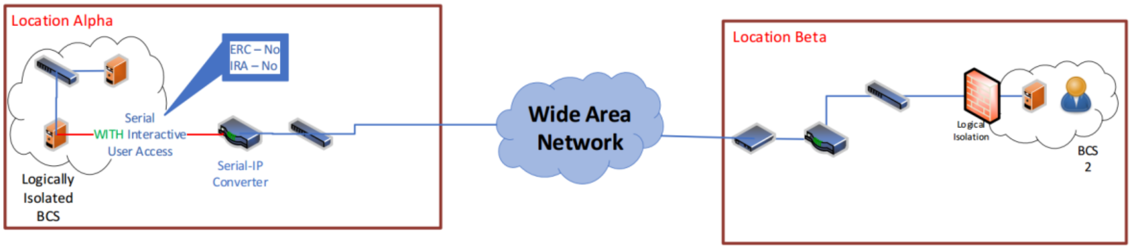
Remote Routable Data



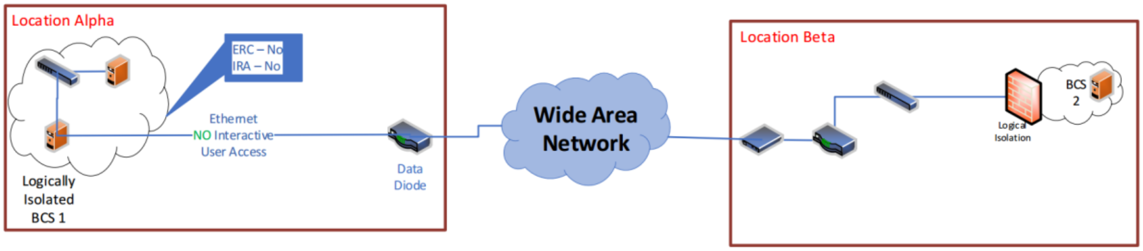
Remote Serial Data



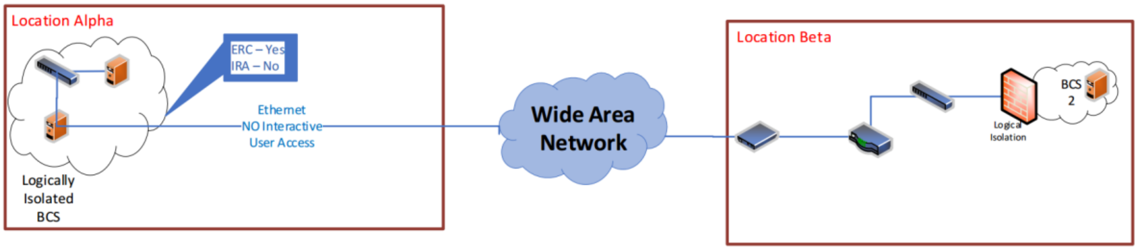
Remote Serial Access From Another BCS



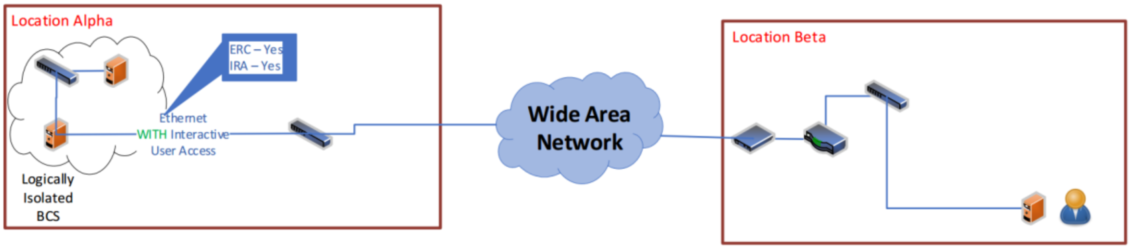
Diode



Remote Routable Data



Remote Routable Access



Assets with Multiple Classifications (PCA, EACS, IS, SCI, etc.)

The definitions created in support of the CIP Standards have historically included overlap. In this current version of CIP-005-7, the definition of PCA is updated with conforming changes that include Virtual Cyber Assets, as well as those that share computer resources with BES Cyber Systems. Additional definitions such as Shared Cyber Infrastructure and Virtual Cyber Asset will add to the possibility of additional instances of assets or systems meeting multiple definitions, such as EACS that are also PCAs, or SCI that is also an EACS.

These definitions are used in both the Applicable Systems column as well as within the language of the Requirement. The fact that one asset or system may have multiple classifications does not pose a significant challenge as long as the Responsible Entity ensures that all Requirements that pertain to ANY of the classifications are applied. In other words, if an asset or system meets both the SCI and the EACS definition, requirements that apply to either definition would be applicable.

Requirement R1

General Considerations for Requirement R1

> **Requirement R1:** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-7 Table R1 – Logical Isolation. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

Rationale

Requirement 1 is designed to implement various forms of logical isolation between systems in different ESPs or ESZs and have the access controlled between them. The ESP model continues unchanged as the 1.2 requirement part moves to an objective-based requirement that the EAP model can meet. However, requirement R1 allows for other models (such as zones and zero-trust models) that can also meet the objective in 1.2. For the ESZ concept, the requirement has new requirement parts to cover what systems can reside in what zones to mitigate the risks of “mixed trust” environments that are possible on shared infrastructure.

Requirement R1 Part 1.1

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	All applicable systems shall reside within one or more defined ESPs or ESZs.	An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems.

Rationale

This requirement part gives the entity the option to use either the ESP model or the ESZ model for implementing the logical isolation of the applicable systems. For a discussion of the ESZ option, see the rationale for the ESZ and SCI definitions above, the General Considerations section above, as well as the diagram depicting various ESZ configurations in Attachment 1.

Requirement R1 Part 1.2

Part	Applicable Systems	Requirements	Measures
1.2	Electronic Security Perimeters and Electronic Security Zones created in Part 1.1.	Require inbound and outbound logical access permissions, including the reason for granting access, and deny all other logical access by default. Excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	An example of evidence may include, but is not limited to, architectural diagrams that detail how network communication is limited and a list of rules (firewall, access control lists, software defined policies, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.

Rationale

Removal of Electronic Access Point (EAP):
The SDT is proposing the removal of EAP as a definition, therefore, the applicability of CIP-005-7 R1.2 also needs to change. The SDT chose ESP(s) and ESZ(s) created in Part 1.1 as the Applicable Systems where Registered Entities are required to apply the inbound and outbound access controls to replace the term EAP. By doing so, current Access Control Lists in-place for established EAPs continue to serve the same purpose and should remain compatible with this requirement part. Also see the discussion of the ESZ and EAP terms above.

Requirement Parity within ESZ to establish security level and address "mixed trust":
The SDT chose to establish the ESZ at a single trust level by assigning the same set of requirements throughout the CIP standards to systems that reside within an ESZ. The goal of this is to minimize the ability of an attacker to pivot from one system to another within an ESZ. An example of this is the threat of an attacker escaping a virtual machine to access the host hypervisor and other Virtual Machines (VMs). If there were systems within the ESZ that were not held to the same trust level, compromising those systems could be potentially easier, which would allow an attacker to pivot and compromise systems to the higher impact targets within the same ESZ.

For example, if a Protected Cyber Asset (PCA) within an ESZ is not subject to the same CIP-004 requirements for personnel accessing the PCA as it is for the BES Cyber Systems within the same ESZ, it could be used as a "pivot" for allowing unauthorized access to the BES Cyber Systems within the ESZ.

In future formal postings of the CIP standards with conforming changes applied, the affected requirements will have "hosted on SCI" phrasing within the "Applicable Systems" column. These requirements establish a single security or trust level for the applicable systems within an ESZ. Each of these requirements serves a specific security need, and if missing, would reduce the security level of the hosted virtualized systems potentially reducing the security level of the associated BCS.

The obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions.

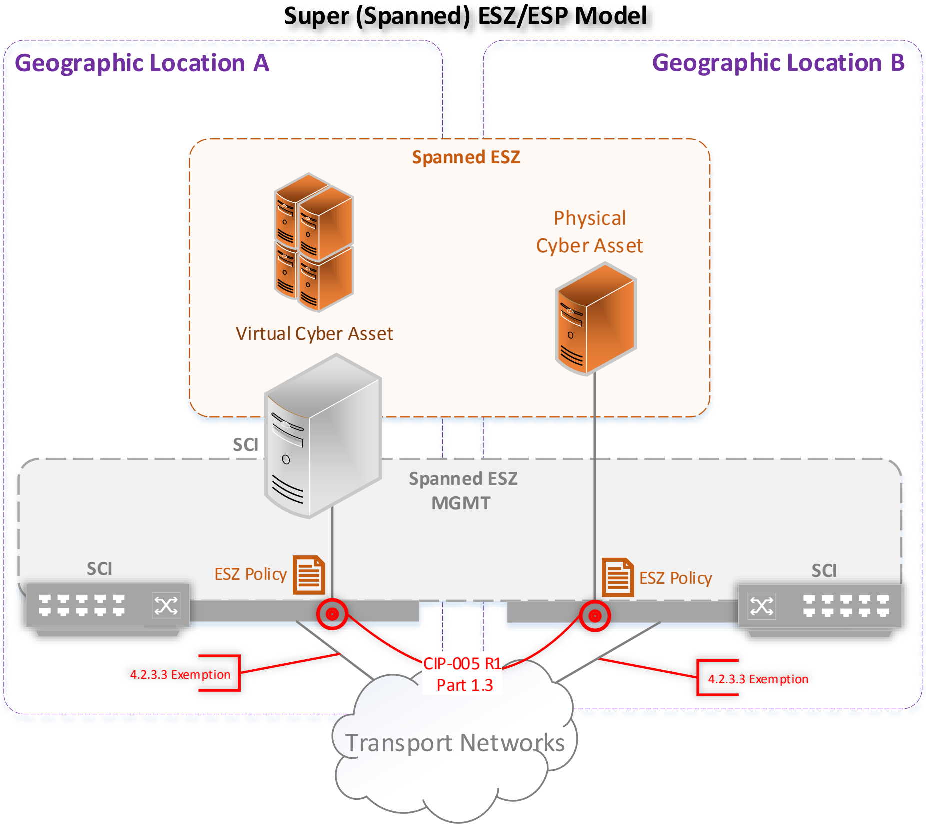
Requirement R1 Part 1.3

Part	Applicable Systems	Requirements	Measures
1.3	Electronic Security Zone or Electronic Security Perimeter that spans more than one geographic location containing: • High Impact BES Cyber Systems • Medium Impact BES Cyber Systems	Protect the confidentiality and integrity of the data traversing communication networks and data communication links used to extend an applicable ESP or ESZ, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	Evidence may include, but is not limited to, architecture documents detailing the methods used to mitigate the risk of unauthorized disclosure. Examples include physical protection and the points where encryption initiates and terminates.

Rationale

Part 1.3 is a new requirement intended to protect the confidentiality and integrity of data flowing between an entity's facilities when that data is contained within a single ESP or ESZ that spans more than one geographic location, commonly referred to as a 'Super ESP.'

One of the issues with the ESP construct carried forward into the logical isolation model is the situation where entities have BES Cyber Systems that include components at separate locations. For example, if an entity has a need to replicate data at high speed between two databases in two different geographic locations to improve the resilience and reliability of BES Cyber Systems, the entity may have issues with the 4.2.3.2 exclusion in the standards that exempts the network and communications gear that is "between discrete ESPs." If the protocol is not routable then no ESP can be created. The entity needs to be able to have a "Super-ESP" that can span more than one location.



The ESP model, along with the 4.2.3.2 exclusion within the CIP standards applicability does not lend itself to this construct. As technology evolves, there will be many more instances where a BES Cyber System may need to span locations. Traditionally this situation could be addressed by installing an EAP at each site as an ESP boundary that would then allow the communications equipment between the sites to be subject to the exemption if routable protocols are used.

The 'Super ESP' construct has been addressed with a new exclusion and a new requirement (CIP-005 R1.3). The new exclusion in 4.2.3.3 allows Cyber Assets associated with communication networks and data communication links used to extend an ESP or ESZ to more than one geographic location to be exempt from the standard since many of these Cyber Assets may be owned by carriers. However, the new R1.3 in CIP-005 requires that data over this exempted communication be protected to preserve its integrity and confidentiality, with the exception of time sensitive protection functions.

The exemption within this requirement part for "Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012" does not exempt it from protection under the CIP standards as it is covered by CIP-012. The intent of this exemption is to keep any issues with CIP-012 compliance from becoming a CIP-005 issue as well if the two control centers in question also have the "Super-ESP" implemented.

Requirement R1 Part 1.4

Part	Applicable Systems	Requirements	Measures
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI •	Perform authentication when establishing Dial-up Connectivity with applicable systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

Rationale

CIP-005-7, Part 1.4 reinforces that dial-up connectivity should perform authentication whenever possible so that the BES Cyber System is not directly accessible with only a phone number. It has been changed to apply to virtualized environments as well and update the TFE requirements to the “per system capability” language.

Requirement R1 Part 1.5

Part	Applicable Systems	Requirements	Measures
1.5	High Impact BES Cyber Systems and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI Medium Impact BES Cyber Systems at Control Centers and their associated: • PCA • SCI • PACS hosted on SCI • EACS hosted on SCI	Have one or more methods for detecting known or suspected malicious routable Internet Protocol (IP) communications to or from ESPs or ESZs.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

Rationale

CIP-005-7 requirement 1.5 reflects the retirement of the term EAP in favor of utilizing the terms ESP and ESZ. The intent of requirement 1.5 is to detect known or suspected malicious communications at the ESP or ESZ boundaries.

The use of "to or from" in the requirement is to solidify where the detection should take place, which is at the boundary of the ESP or ESZ and not communications within the ESP or ESZ. The use of the phrase “routable Internet Protocol (IP) communications” is intended to eliminate internal storage transport protocols including, but not limited to Fibre Channel, iSCSI, and InfiniBand from the scope of this requirement as well as serial communications.

The change in the applicable systems is to provide both forward and backward compatibility within the same requirement.

Requirement R1 Part 1.6

Part	Applicable Systems	Requirements	Measures
1.6	Shared Cyber Infrastructure that hosts High Impact BES Cyber Systems Shared Cyber Infrastructure that hosts Medium Impact BES Cyber Systems	Management systems may only share CPU, memory, and ESZ or ESP with other management systems and the management plane.	Examples of evidence may include, but is not limited to, documentation that includes the configuration of systems that enforce authentication and isolation such as: • Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS) • Physical isolated out-of-band network for dedicated management interfaces, embedded management interfaces • Compute configuration showing the isolation of the management plane resources (e.g., hypervisor, containers)

Rationale

The SDT is proposing a new Requirement, CIP-005-7 Requirement R1, Part 1.6. The purpose of this new Requirement is to separate the management plane of SCI from the data plane.

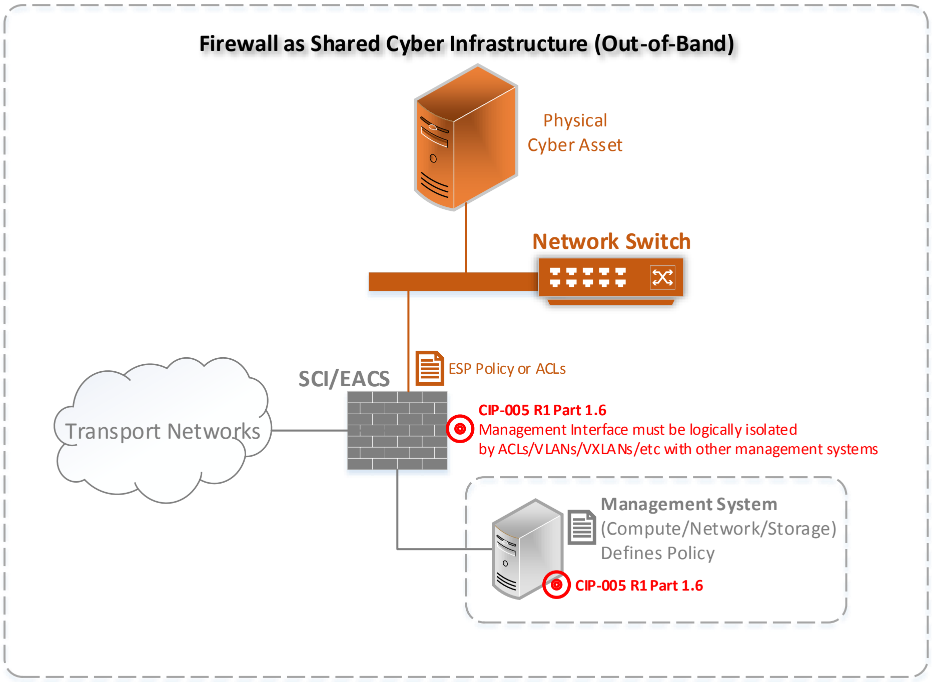
As virtualized servers, networks, switches, firewalls, and storage are logical constructs, controlling access and communications to the management plane of these systems becomes imperative. Access to the management plane (interface, console, etc.) allows users to create, modify, or delete objects or entire infrastructures, or move objects from one zone or network to another. Therefore, administrative level or “management plane” access to the SCI is critical to the security and reliability of the hosted systems. By isolating the management interface of these devices from the larger audience of users that can access the data plane, the threat base is reduced to the group of users with access to the administrative functions.

The methods used to separate the management plane from the data plane developed quickly as systems moving to the cloud increased. For a cloud-based hosting facility to be successful, the tenants must share hardware resources (SCI as defined here) but have no ability to access or modify other tenants or their configuration. Cloud technology was forced to enhance existing methods and develop new methods to accomplish this separation.
SCI presents the same issue for in-house (on-premise) virtualization environments. CIP-005 R1.6 will mitigate that issue by bringing the isolation of the management plane into the scope of the CIP standards. This is accomplished by requiring that entities allow management systems to share CPU and memory (e.g. hypervisors) only with other management systems. It also requires that management systems share an ESZ only with other management systems.

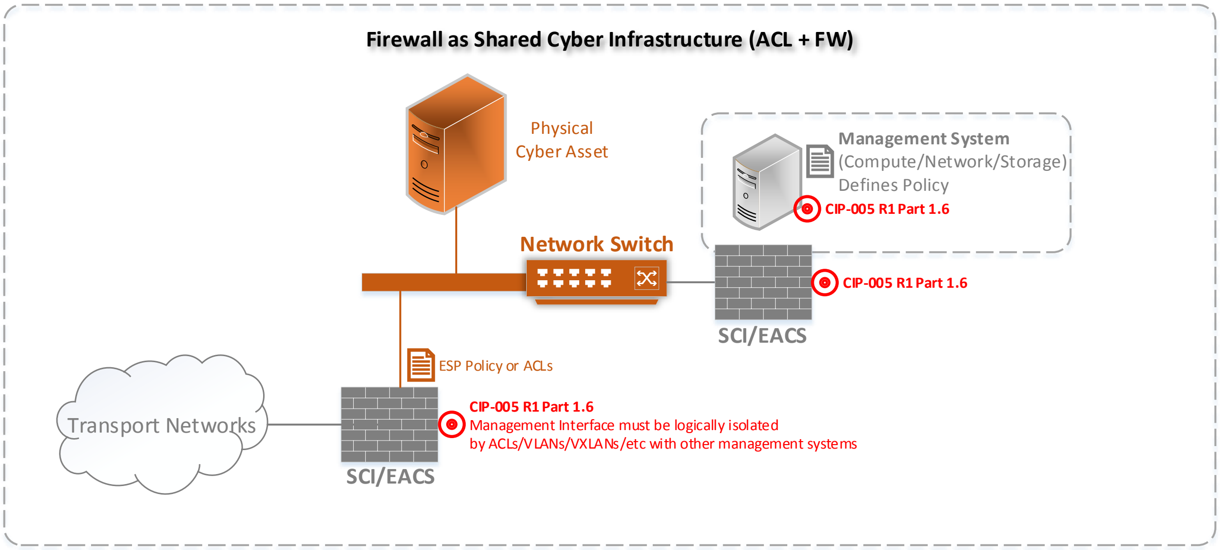
Because hypervisors give us the ability to use affinity rules to determine what VMs use what resources, affinity and anti-affinity rules are a critical part of the isolation solution for management systems hosted on SCI. An affinity rule will ensure a group of virtual machines are only allowed to reside on a group of hypervisors. The use of an anti-affinity rule will ensure another group of VMs cannot reside on the group of hypervisors reserved in the previous affinity rule. While different hypervisors have different methods for achieving this, the idea is the same across all mass market hypervisors.

The statement "or performs logical isolation for an ESZ or ESP" is found within the Shared Cyber Infrastructure definition. This inclusion is intended to ensure that devices that provide logical isolation for an ESZ or ESP have protection for the associated management systems (management plane). This inclusion means the management plane of firewalls or network switches that provide logical isolation to an ESP, ESZ, or within Shared Cyber Infrastructure now fall within scope of R1.6. It is not intended for network switches that are part of a system and are not providing logical isolation between ESPs or ESZs. The following diagrams outline numerous options that help to further clarify the intent of R1.6 as it applies to firewalls and network switches that implement ESP or ESZ logical isolation.

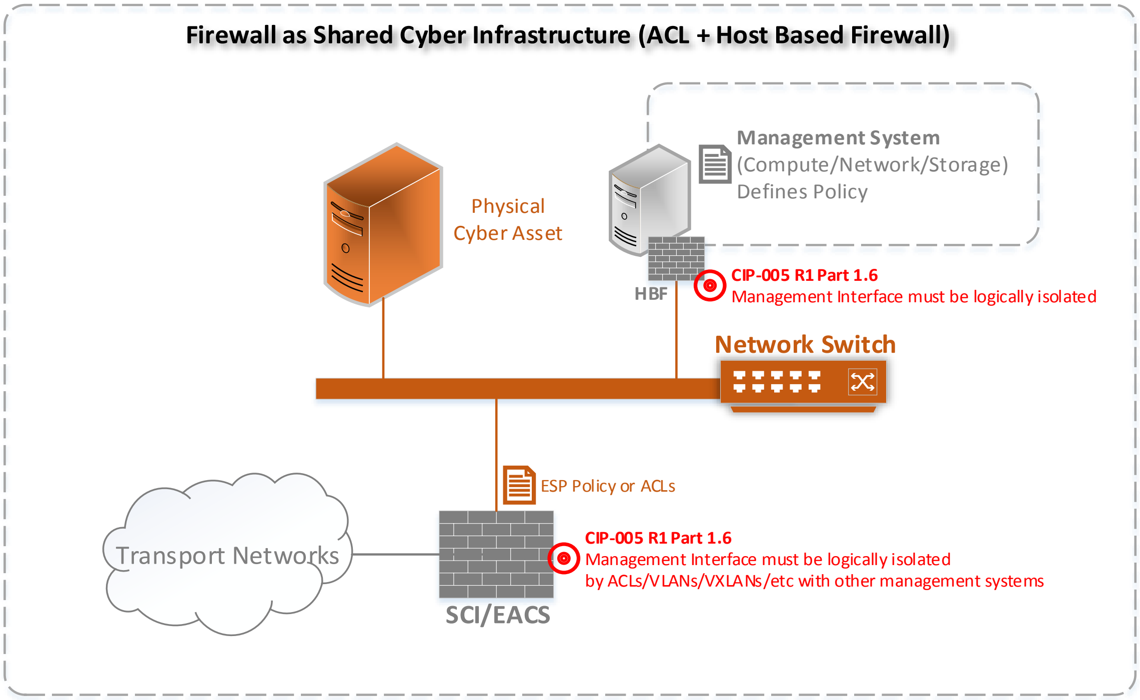
The option below shows the typical out-of-band management of the SCI by putting the management system on a separate interface. This keeps the management system in an ESP or ESZ not shared with other non-management systems. The network switch is not used to perform logical isolation.



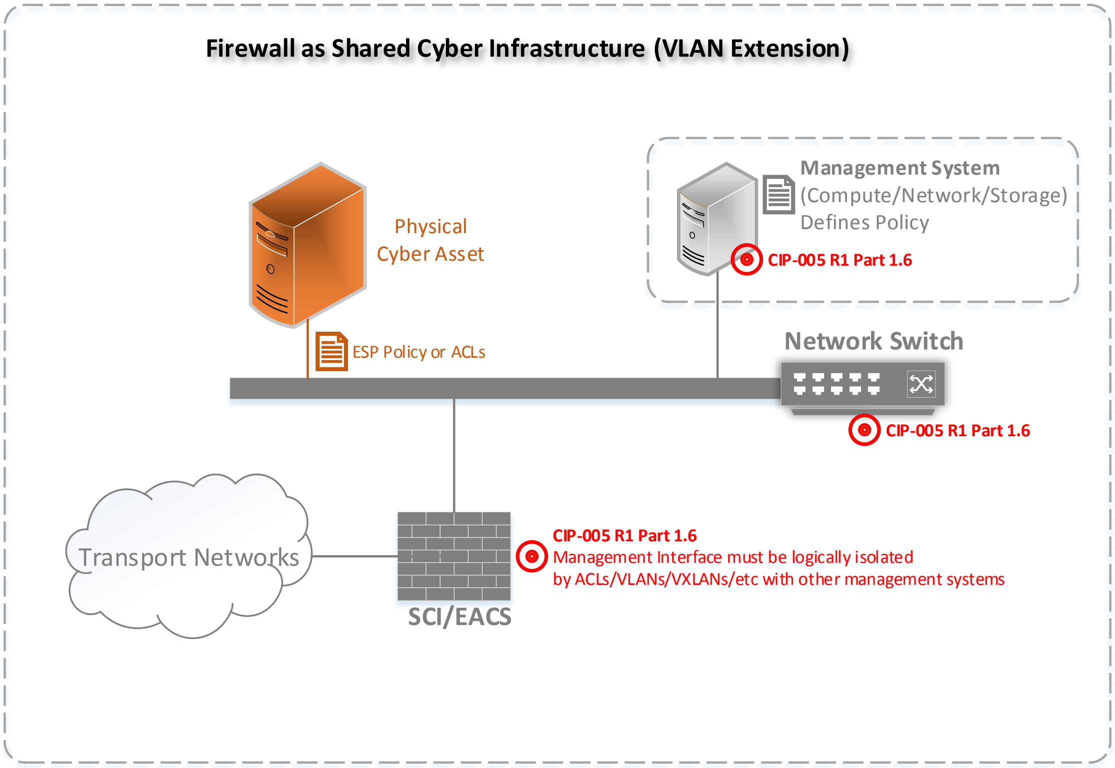
The option below depicts a management system that is located at a site with one network switch. Some sort of logical isolation is required so that the management system is not visible to those with access to the Cyber Asset on the same switch. Another firewall is implemented here to put the management system in an ESP or ESZ separate from the other Cyber Assets. The network switch is not used for logical isolation.



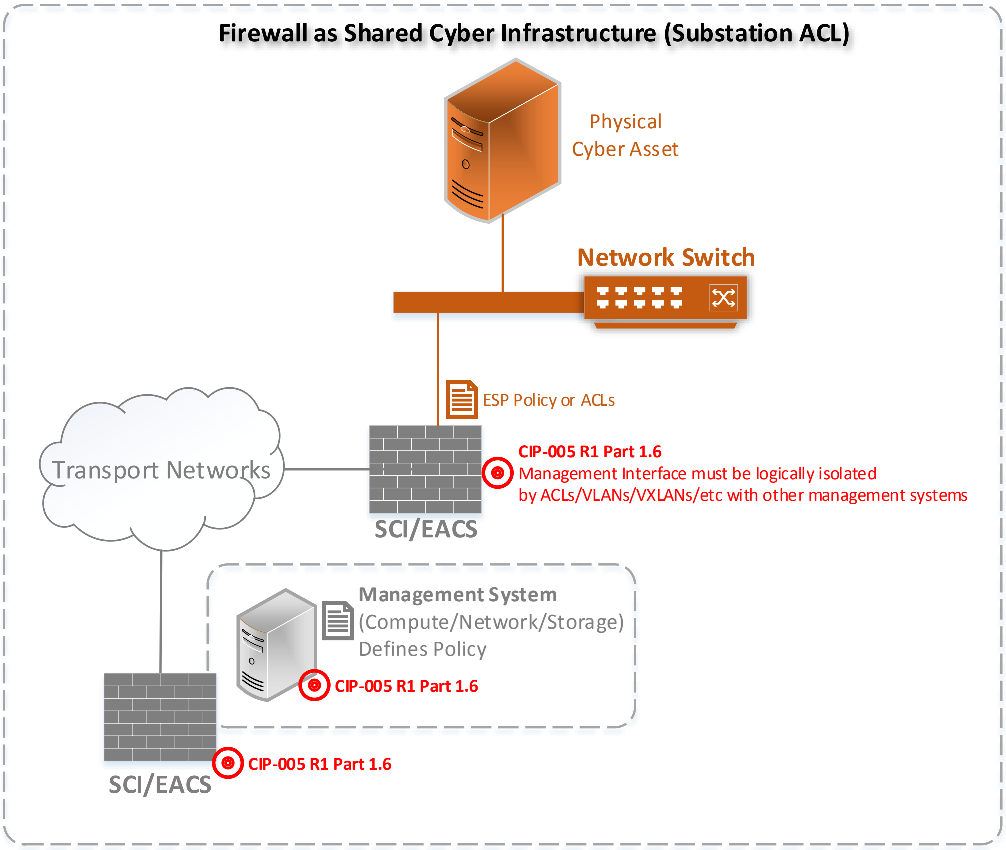
In the option below, the same situation exists, but instead of a separate physical firewall a host based firewall is used on the management system to logically isolate it.



In the option below, the management system is connected to the network switch and the switch is used for the logical isolation. Virtual LANs (VLANs) are configured in the switch along with ACL's in the firewall in order to implement the two different ESZs to isolate the management system. The network switch itself now also becomes SCI and it's management plane now must be in the management ESZ as well.



In the option below, a centralized management system is depicted at another location. ACLs are implemented in the intervening firewalls (SCI) such that the access to the management plane of those firewalls is only allowed to the centralized management system.



Requirement R2

> *R2.* Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-7 Table R2 –Remote Access Management* for all remote access that originates from outside of any of the entities' ESP's or ESZ's containing high or medium impact BES Cyber Systems or associated SCI. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*

General Considerations for Requirement R2.

Rationale

This requirement added wording for ESZs containing either high or medium impact BES Cyber Systems or associated SCI to provide the equivalent logical protections for remote access that existed before. The wording for existing ESPs was retained for backward compatibility purposes to CIP-005-6.

Previously, the applicability of the remote access was included within the definition of IRA, which included access that did not originate from within another of the entity's ESPs. That applicability has been removed from the definition (see discussion of IRA above) and placed within the requirement so that the definition does not need to change when the applicability of a requirement that uses it changes.

Requirement R2 Part 2.1

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: • PCA • SCI Medium Impact BES Cyber Systems with IRA and their associated: • PCA • SCI	Ensure that Interactive Remote Access is through an Intermediate System that is not inside an applicable ESP or ESZ.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.

Rationale

The Applicable Systems section of this requirement was updated to include SCI associated with high and medium impact BES Cyber Systems. This was done to ensure that same safeguards for remote access methods and technologies exist for the applicable SCI as the high and medium impact BES Cyber Systems and associated PCA's being hosted on that SCI. Backwards compatibility with CIP-005-6 is maintained for entities that do not currently use SCI.

For Medium Impact BES Cyber Systems, the Applicable Systems wording was updated from "with External Routable Connectivity" to "with IRA". This was done to cover serial connectivity associated IRA for those applicable systems without External Routable Connectivity (ERC). This aspect of IRA was missing from earlier versions of CIP-005. This change is intended to mitigate risks associated with a possible external (to the entity) attack vector in situations where serial connectivity is converted to network connectivity using a terminal server type device. This is one of the issues noted by the V5TAG. Please refer to the section of this document entitled "External Routable Connectivity (ERC) and Interactive Remote Access (IRA)."

The inclusion of the wording for "associated SCI" is intended to target the management plane of the associated SCI. This is to ensure that the management plane of the SCI being used to support BES Cyber Systems is also protected in an equivalent manner.

Backwards compatibility with CIP-005-6 is maintained except in the above situations.
The requirement language itself was simplified. Note that the definitions of IRA and IS have been updated. Please note that the definition of IRA was changed to include serial communications connections. This change maintains backwards compatibility with CIP-005-6 except where serial connectivity is being used for IRA.
The required location of an Intermediate System was within the definition previously. The definition of IS has been simplified and its required location (not inside an applicable ESP or ESZ) is now within the requirement rather than the definition.

Requirement R2 Part 2.2

Part	Applicable Systems	Requirements	Measures
2.2	Intermediate Systems associated with High Impact BES Cyber Systems. Intermediate Systems associated with Medium Impact BES Cyber Systems.	Protect the confidentiality and integrity of Interactive Remote Access between the client and the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

Rationale

The Applicable *Systems* was changed to IS from high or medium BES Cyber Systems and associated PCA's. This change better reflects that this requirement is associated with the IS itself.

The requirement was changed from a specific technical based requirement for encryption to an objective based requirement to protect the IRA session. The proposed language of this requirement takes into account the possibility that other equally effective methods could be developed and deployed. This also prevents outdated encryption methods from being utilized.

The changed requirement is backwards compatible with the CIP-005-6 except where outdated encryption methods have been used.

Requirement R2 Part 2.3

Part	Applicable Systems	Requirements	Measures
2.3	Intermediate Systems associated with High Impact BES Cyber Systems. Intermediate Systems associated with Medium Impact BES Cyber Systems.	Require multi-factor authentication to IS.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

Rationale

The Applicable Systems was changed to IS from high or medium BES Cyber Systems and associated PCA's. This change better reflects that this requirement is associated with the IS itself. Note that serial connection-based IRA is now included due to the IRA definition change. The requirement itself was not changed.

The changed requirement is backwards compatible with the CIP-005-6 except where serial connection-based IRA is being utilized.

Requirement R2 Parts 2.4 – 2.5

Part	Applicable Systems	Requirements	Measures
2.4	High Impact BES Cyber Systems and their associated: - PCA - SCI - PACS hosted on SCI - EACS hosted on SCI Medium Impact BES Cyber Systems and their associated: - PCA - SCI - PACS hosted on SCI - EACS hosted on SCI -	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: - Methods for accessing logged or monitoring information to determine active vendor remote access sessions; - Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or - Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High Impact BES Cyber Systems and their associated: - PCA - SCI - PACS hosted on SCI - EACS hosted on SCI Medium Impact BES Cyber Systems and their associated: - PCA - SCI - PACS hosted on SCI - EACS hosted on SCI -	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: - Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or - Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

Rationale

The Applicable Systems section was changed to include associated SCI, PACS hosted on SCI, EACS hosted on SCI, EAMS hosted on SCI. This change is needed due to the possibility of "differing trust levels" when these types of assets utilize the same SCI. Please refer to the section in this document entitled 'Shared infrastructure and "Mixed Trust" Risks'. In summary, this change is intended to mitigate the risk associated with "side channel" based attack vectors where it could be possible to compromise one virtual cyber asset and then subsequently access the any other virtual cyber asset running on the same SCI. Also note that serial connection-based IRA is now included due to the change in the definition of IRA.

The inclusion of the wording for “associated SCI” is intended to target the management plane of the associated SCI. This is to ensure that the management plane of the SCI being used to support BES Cyber Systems is also protected in an equivalent manner

The requirements themselves have not been changed. Note that the requirement includes both vendor based IRA and system-to-system access.

Note that the changes to applicable systems only applies to those virtual cyber assets hosted on the same SCI. These changes don’t apply where SCI is not utilized. These changed requirements are backwards compatible with the CIP-005-6 except where SCI is currently being utilized and where serial connection-based IRA is being utilized.

Requirement R2 Part 2.6

Part	Applicable Systems	Requirements	Measures
2.6	Intermediate Systems that are hosted on SCI and are associated with High Impact BES Cyber Systems. Intermediate Systems that are hosted on SCI and are associated with Medium Impact BES Cyber Systems.	IS may only share CPU, memory, and ESZ or ESP with other IS.	An example of evidence may include, but is not limited to, documentation that includes the following: configuration showing that the CPU and memory can only be shared with other IS.

Rationale

This is a new requirement that only applies to IS hosted on SCI. This new requirement is proposed due to the possibility of:

- IS being used by external parties outside of the entities such as vendors; and,
- IS being accessible to external connections outside of the entity such as entity support staff utilizing IRA across an internet connection to support a remote site.

Please refer to the section in this document entitled “Shared infrastructure and “Mixed Trust” Risks” and the subsequent discussion on “affinity”. The new requirement is for “affinity” and a separate ESZ.

In summary, this new requirement is intended to mitigate the risk associated with “side channel” based attack vectors where it could be possible to compromise the IS from an external source and then subsequently access the any other virtual Cyber Asset running on the same SCI.

As this is a new requirement only applies to IS hosted on SCI, it is backwards compatible with the CIP-005-6 except where SCI is currently used.

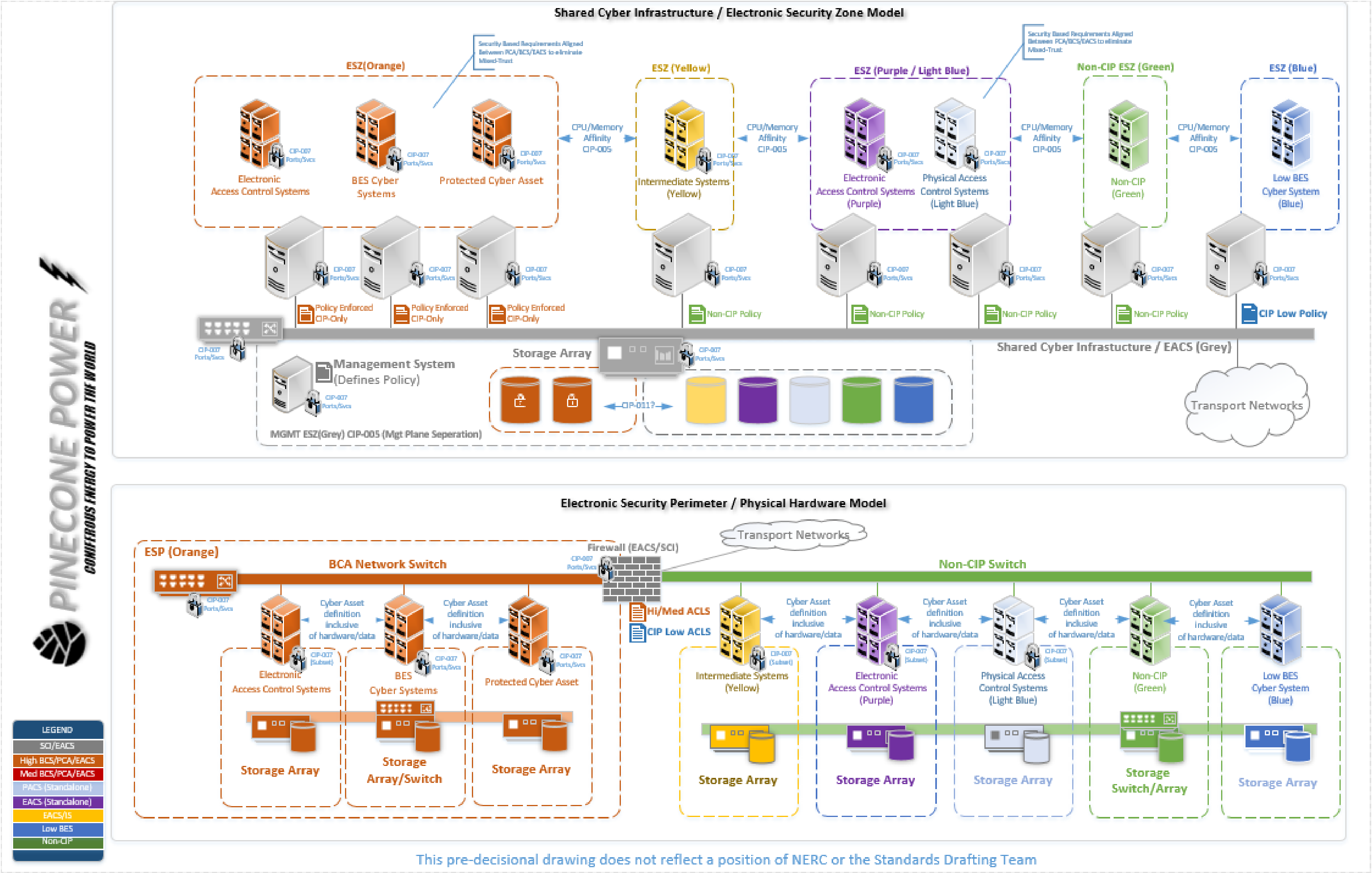
Appendix 1 – ESZ's

This section contains a diagrams for a fictional utility company ("Pinecone Power").

Figure 1 is used to show a virtualized scenario at the top of diagram and contrasts it with a typical physical hardware model on the lower half. The virtualized scenario fully utilizes the ESZ concept and has practically every kind of system hosted within the environment. The color coding (see legend at lower left) depicts the categorization of various components. The diagram shows the different ESZs that would be required and the affinity rules that would be needed between them such that systems of different security levels would not share the same hypervisor with systems in other zones.

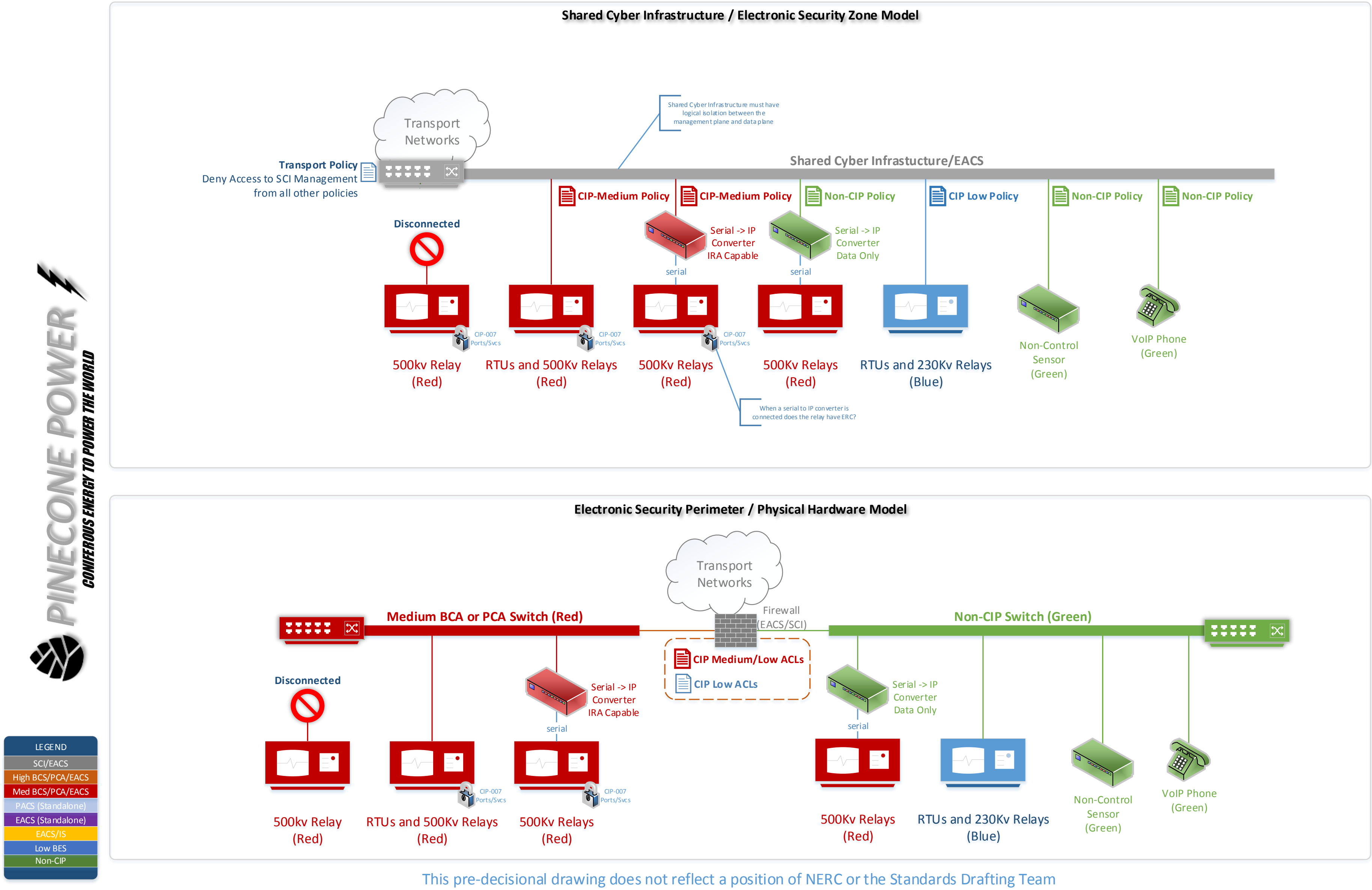
Figure 2 is used to describe substation and plant hybrid virtualization scenarios. It also uses the ESZ concept to secure devices connected to the switch.

Figure 1



This pre-decisional drawing does not reflect a position of NERC or the Standards Drafting Team

Figure 2



This pre-decisional drawing does not reflect a position of NERC or the Standards Drafting Team

Appendix 2 - Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber

Assets within the ESP, even other BES Cyber Systems of lesser impact, as “Protected Cyber Assets” of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an “Associated Protected Cyber Asset” of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually ‘command and control’ hosts on the Internet, or compromised ‘jump hosts’ within the Responsible Entity’s other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT’s intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity’s address space. The SDT’s intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and ‘deny by default’ type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear ‘perimeter type’ security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions (“TFEs”) rather than increased security.

As for dial-up connectivity, the Standard Drafting Team’s intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:
See Secure Remote Access Reference Document (see remote access alert).

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)

Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)

Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)

Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)

Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)

Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement UPDATE

2016-02 Modifications to CIP Standards
CIP-005 and Associated Definitions

Informal Comment Period Open through September 26, 2019

Now Available

The informal comment period for the **Virtualization Updates for CIP-005 and Associated Definitions** has been extended an additional 15 days and is now open through **8 p.m. Eastern, Thursday, September 26, 2019.**

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Wendy Muller regarding issues using the SBS. An unofficial Word version of the comment form is posted on the project page.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The drafting team will review all responses received during the comment period and determine the next steps of the project**.**

For more information on the Standards Development Process, refer to the Standard Processes Manual.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Applications" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box. For more information or assistance, Jordan Mallory (via email) or at (404) 446-2589.

Comment Report

Project Name: 2016-02 Modifications to CIP Standards | Virtualization Updates for CIP-005 and Associated Definitions

Comment Period Start Date: 8/9/2019

Comment Period End Date: 9/26/2019

Associated Ballots:

There were 54 sets of responses, including comments from approximately 135 different people from approximately 108 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT is proposing the new Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions to allow requirements to be specifically targeted at virtualized environments. The SDT is also proposing conforming changes in several other definitions to allow VCA's as an option. Do you agree with the development of new terms and the proposed definition of those terms? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (NOTE: Future CIP-011 requirements to be developed to address logical isolation within storage systems and will be coordinated with Project 2019-02 (BCSI)). (CIP-005 Technical Rationale pages 11-12).

2. The CIP SDT tried to maintain backwards compatibility throughout CIP-005. However, in order to take advantage of emergent technologies the existing firewall that were associated with an EAP will now fall into the SCI definition and be subject to CIP-005 Requirement R1 Part 1.6, which requires management plane separation. What level of effort would be required to accommodate these changes? Do you agree? If not, please provide comments to support your response. (CIP-005 Technical Rationale pages 11, 13, and 29-32).

3. The SDT is proposing the new term Electronic Security Zone (ESZ) to enable future technologies such as policy based environments. Do you agree with the proposed definition? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. Note: ESP will be retained for backwards compatibility. (CIP-005 Technical Rationale pages 10, 14-18, 22-26, and 38-40).

- **Electronic Security Zone (ESZ): A segmented section of a network that contains systems and components to create logical isolation.**

4. The SDT is addressing the risk of systems of different impact, trust, or security levels ("mixed trust") environments that are possible on Shared Cyber Infrastructure by modifying the definition of Protected Cyber Asset (PCA) so that it includes those VCA's that can share a hypervisor's CPU or memory. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 8, and 14-15).

5. The SDT proposes to address infrastructure that is shared between differing BCS impact ratings that share CPU and memory resources by aligning the CIP Requirements for all systems within an ESZ or ESP and affinity to prevent sharing of CPU and memory between Virtual Cyber Assets of differing impact ratings. Do you agree with these changes? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 11, 12, and 14).

6. The SDT is proposing the addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3 for "Super-ESP" scenarios where single ESP's or ESZ's span multiple geographic locations. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 18, and 25-26).

7. The SDT is proposing to retire EACMS and develop two new terms: EACS and EAMS. These terms will allow changes within the applicable systems column of the relevant requirements to allow third party monitoring. Monitoring and logging data will be handled within CIP-011 in a future posting. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. NOTE: Project 2016-02 will coordinate with Project 2019-02 (BCSI) and Project 2019-03 (Supply Chain) on this topic. (CIP-005 Technical Rationale pages 9, 10, 13, and 19).

8. The V5TAG document request the SDT to "Clarify the IRA definition to address the placement of the phrase "using a routable protocol" in the definition and clarity with respect to Dial-up Connectivity." Therefore, the SDT proposes modifications to the IRA definition and CIP-005 Requirement R2. These modifications will clarify scenarios where Interactive Remote Access applies to serial only devices. Do you agree? If

you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 7, 19-21, 27, and 33-37).

9. The SDT is proposing modifications to CIP-005 Requirement R1. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rational pages 22-32).

10. The SDT is proposing modifications to CIP-005 Requirement R2. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rationale pages 33-37).

11. Backwards Compatibility: What level of effort is required to migrate from existing definitions to new definitions on existing virtualized architecture?

12. The SDT posted a draft CIP-005-7 Technical Rationale document to explain the basis behind these proposed changes. Please provide any additional comments on this document

13. Provide any additional comments for the SDT to consider, if desired

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aubrey Short	1,3,4		Aubrey Short, On Behalf of:	aubrey short	FirstEnergy	4	RF
					Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Andy Crooks	SaskPower Corporation	1	MRO
					Bryan Sherrow	Kansas City Board of Public Utilities	1	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO

					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					David Zwergel	Midcontinent ISO	2	MRO
					Douglas Webb	Kansas City Power & Light	1,3,5,6	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					James Nail	Independence Power & Light (Indepdence Missouri)	1,3,5	MRO
					James Williams	Southwest Power Pool, Inc.	2	MRO
					Jamie Monette	Minnesota Power / ALLETE	1	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Sing Tay	Oklahoma Gas & Electric	1,3,5,6	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Troy Brumfield	American Transmission Company	1	MRO
Public Utility District No. 1 of Chelan County	Davis Jelusich	1,3,5,6		Public Utility District No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC

PPL - Louisville Gas and Electric Co.	Devin Shines	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					JULIE HOSTRANDER	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
Great Plains Energy - Kansas City Power and Light Co.	Douglas Webb	1,3,5,6	MRO,SPP RE	Westar-KCPL	Doug Webb	Westar	1,3,5,6	MRO
					Doug Webb	KCP&L	1,3,5,6	MRO
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					John Shaver	Arizona Electric Power Cooperative	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Tara Lightner	Sunflower Electric Power Corporation	1	MRO
					Colette Caudill	East Kentucky Power Cooperative	1,3	SERC
Duke Energy	Masuncha Bussey	1,5,6	FRCC,RF,SERC	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Southern Company - Southern	Pamela Hunter	1,3,5,6	SERC	Southern Company	Adrianne Collins	Southern Company - Southern	1	SERC

Company Services, Inc.						Company Services, Inc.		
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC		RSC no NGrid and Eversource	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Sean Cavote	PSEG	4	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					David Kiguel	Independent	NA - Not Applicable	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC

					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Mike Forte	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Ashmeet Kaur	Con Ed - Consolidated Edison	5	NPCC
					Caroline Dupuis	Hydro Quebec	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Laura McLeod	NB Power Corporation	5	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC

					Gregory Campoli	New York Independent System Operator	2	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	3,5,6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable

1. The SDT is proposing the new Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions to allow requirements to be specifically targeted at virtualized environments. The SDT is also proposing conforming changes in several other definitions to allow VCA's as an option. Do you agree with the development of new terms and the proposed definition of those terms? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (NOTE: Future CIP-011 requirements to be developed to address logical isolation within storage systems and will be coordinated with Project 2019-02 (BCSI)). (CIP-005 Technical Rationale pages 11-12).

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

Unsure if SCI is including the hypervisor as there is an inclusion for "management systems". PSP: Definition needs to provide a scope of what is being protected. Current definition has BCA, BCSs…IS should have clearer distinction from an EACS. An IS should be a Cyber Asset that does not provide the electronic access control of an EACS, but a Cyber Asset that is a jumpbox into an ESP/ESZ.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

1). We disagree with a separate VCA definition. Any requirement should be allowable to apply to virtual and physical CIP Cyber Assets for the consistency as long as it is applicable. If the Cyber Asset definitions is split into two separate ones, you may have to specify which requirements apply to virtual CIP Cyber Assets and which requirements apply to physical CIP Cyber Assets and then the applicable system will become more complicated such as Virtual BCA, Physical BCA , Virtual EACMS and Physical EACMS, etc. We suggest modifying Cyber Asset definition to include the virtual cyber asset as follows:

"A programmable electronic or virtual devices, including the hardware or virtual hardware, software, and data in those devices, where a virtual device is a logical instance of an operating system, firmware, or self-contained application hosted on a physical device. Each virtual machine and host is a distinct device."

2). We disagree with SCI definition. The following are the rational for not defining the SCI:

a) Hypervisor Host and Management Plane Device

· If the VM is a BCA, its hypervisor host and management plane (e.g., vCener) should be identified as BCA devices since they can delete and modify the VM within 15 minutes and meet the BCA definition.

· If the VM is an EACMS or PACS, its hypervisor host and management plane should be identified as EACMS or PACS devices since they can delete and modify the virtual EACMS or PACS resulting in removing or changing the electronic/physical access control functions and meet the EACMS or PACS definition. For ensuring that the hypervisor host and management plane devices are identified correctly, we suggest modifying the definition of EACMS and PACS as follows:

EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes the Cyber Assets that can create, modify or delete the said Cyber Assets and Intermediate Systems”

PACS: “Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. This includes the Cyber Assets that can create, modify or delete the said Cyber Assets.”

b) Storage Device and SAN

If the storage device or SAN is used for VM running rather than backing up information, the storage device should be considered a part of the VM since the VM cannot run without it. Any requirements that apply to the VM should also apply to the storage device and SAN network.

Based on the above rationale, given that the SCI falls within the existing definition of BCA, EACMS or PACS, the SCI definition is not needed.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT agrees with the concepts of the new definitions. However, it raises the following issues with the definitions:

SCI: Consider rewording as “storage and its associated network transport” and providing clarification on how a switch within an ESP should be classified under this new construct.

VCA: The definition does not address “data” consistent with the Cyber Asset definition.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company appreciates the opportunity to provide feedback on the SDTs current proposals. We support the SDT efforts to enable registered entities to utilize virtualization within their NERC CIP Cyber Security Programs. While we recognize that current auditing and enforcement of such practices is inconsistent across the regions, this latest approach is another positive step forward to finding secure solutions for the use of virtualization technologies that provide ultimate benefit to Entities and reliability. In support of these positive steps forward, Southern provides the following comments and suggestions in seeking additional clarity on new defined terms and applicability of new requirements.

Southern asks the SDT to consider the following changes to the Shared Cyber Infrastructure definition:

Shared Cyber Infrastructure (SCI): Programmable electronic devices, and their management systems, hosting a Virtual Cyber Asset whose compute, storage (including network transport), or network resources are shared with one or more other Virtual Cyber Assets.

Virtual Cyber Assets (VCA): A logical instance of an operating system, firmware, or self-contained application hosted on Shared Cyber Infrastructure.

This proposed definition change removes the statement “or that perform logical isolation for an ESZ or ESP” in order to delineate between the ability to maintain physical devices to perform logical isolation or alternatively, to use virtual devices to perform logical isolation. For those that choose to utilize physical devices (EACS) and their management systems (EACS) to perform logical isolation, the proposed definition changes may help keep them clearly scoped differently from virtual assets used for the same purpose. Additionally, it should be considered that any Cyber Asset or Virtual Cyber Asset that performs logical isolation for an ESZ or ESP meets the definition of being an EACS, and therefore does not have to also be included in the definition of Shared Cyber Infrastructure – the EACS itself will either be physical or virtual.

Southern asks the SDT to consider a potential conflict between the proposed R1.1 requirement where “All applicable systems shall reside within one or more defined ESPs or ESZs”, and includes EACS hosted on SCI as an applicable system; yet, the proposed R2.1 requirement states “Ensure that all Interactive Remote Access is through an Intermediate System that is not inside an applicable ESP or ESZ.” Given that Intermediate Systems (IS) are also classified as EACS, it would be impossible to require all IS-EACS to be in an ESZ (R1.1) and not (R2.1) at the same time.

Southern also seeks additional clarity on the use of the Applicable System “High Impact BES Cyber Systems and their associated: EACS hosted on SCI”. Is it the intent of the SDT that EACS (or PACS) hosted on SCI and associated with a h/m impact BCS be subject to the requirement even if there are no BCS hosted on the same SCI? Or is the intent for the requirement to only apply to EACS (or PACS) hosted on SCI and associated with a h/m impact BCS when that h/m BCS is hosted, but logically isolated, on the same SCI? As currently written, the latter does not appear to be the case, and the SDTs intention here should be made clearer through modification of the applicability of SCI, and EACS and PACS – whether hosted on SCI with a h/m BCS or not.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

PNM Resources appreciates the effort of the SDT and getting this product out for informal comment. We support the direction the SDT would like to go. Thus our comments are intended to help give feedback to the SDT so a better product can be produced.

We agree with the VCA term and the conforming changes to other definitions to support the term.

We disagree with the definition for Shared Cyber Infrastructure (SCI). The first two of three parts are acceptable, “Programmable electronic devices whose compute, storage (including network transport), or network resources are shared with one or more Virtual Cyber Assets….” It is the third part that is a problem, “or that perform logical isolation for an ESZ or ESP.” A device performing logical isolation is by definition an EACS, “Cyber Assets or Virtual Cyber Assets that provide electronic access control to an ESP, ESZ or BES Cyber System.” It seems redundant to redefine it here. Also, the third bullet results in infinite recursion of CIP-005 R1.1 where SCI as an applicable system shall reside within one or more defined ESPs or ESZ. If the device is providing isolation, then by definition it cannot reside fully within the boundary. You can simply remove the third part and include EACS where ever SCI is also an applicable system and the requirement is addressing a risk to the EACS. It is unclear what risk are attempted to be mitigated for an EACS that perform logical isolation for an ESZ or ESP.

With regard to SCI definition including “management systems” it is unclear what management systems are. The standards and rationale refer to the management plane. So for clarity the SDT should define what it believes management systems are with an official definition.

We agree with PACS, PAMS, EACS, and EAMS along with the retirement of EAP and EACMS.

We believe PCA may need to be revised in the third bullet regarding the sharing of compute resources. The third bullet would be better phrased as “Share computing resources (CPU or memory) with Shared Cyber Infrastructure hosting a BES Cyber Asset.” Currently by proposed definition a BCA excludes SCI and a BES Cyber System is a grouping of BES Cyber Assets. Thus you would never have a PCA on BES Cyber System by definition.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
These new terms and definitions should not only address CIP-005-7, but all CIP standards that would be impacted by virtualization. All standard updates should occur concurrently. The efforts for the entities to adopt these changes would be significant. Also, the proposed definition for PCA is too broad that could potentially bring many more assets into CIP scope.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Dominion Energy supports EEI comments and shares the concerns regarding the ESZ definition.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
VCA – agree with proposed definition.	

SCI – request clarification on what is meant by “its management systems.”

In the SCI definition - Recommend deleting “or ESP” to confine SCI to virtualized firewalls for ESZs, allowing non-virtualized firewall hardware to be solely classified as EACS and not require dual categorization as both EACS and SCI.

Also recommend retaining the EAP definition (at least within the Glossary of Terms) as a useful and necessary term for management of ESPs, but have no objection to the removal of EAP from R1.2 to accommodate virtualization. Note: If EAP is to be removed, also need to remove the reference in VSL Table under R1 on p. 17.

IRA definition change – this revision to the definition goes beyond what is necessary for a conforming change and what was requested and authorized by the SAR (see Question 8).

The SAR recommends improving clarity within the IRA definition of the phrase “using a routable protocol” with respect to Dial-up Connectivity. This could most easily be addressed by simply changing the phrase to “using a routable or dial-up protocol.”

We agree with EEI comments that changes to the IRA definition should be limited to modifying the phrase to “using a routable or dial-up protocol.”

Likes 0	
Dislikes 0	

Response

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO

Answer	No
Document Name	

Comment

VCA – agree with proposed definition.

SCI – request clarification on what is meant by “its management systems.”

In the SCI definition - Recommend deleting “or ESP” to confine SCI to virtualized firewalls for ESZs, allowing non-virtualized firewall hardware to be solely classified as EACS and not require dual categorization as both EACS and SCI.

Also recommend retaining the EAP definition (at least within the Glossary of Terms) as a useful and necessary term for management of ESPs, but have no objection to the removal of EAP from R1.2 to accommodate virtualization. Note: If EAP is to be removed, also need to remove the reference in VSL Table under R1 on p. 17.

IRA definition change – this revision to the definition goes beyond what is necessary for a conforming change and what was requested and authorized by the SAR (see Question 8).

The SAR recommends improving clarity within the IRA definition of the phrase “using a routable protocol” with respect to Dial-up Connectivity. This could most easily be addressed by simply changing the phrase to “using a routable or dial-up protocol.”

We agree with EEI comments that changes to the IRA definition should be limited to modifying the phrase to “using a routable or dial-up protocol.”

Likes 0	
Dislikes 0	

Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	

AEP is appreciative of the Standards Drafting Team’s efforts to consider concerns within the industry during this informal comment period. We are thankful for the opportunity to provide feedback on the modifications currently being proposed.

While AEP holds the opinion that these proposed changes are a step in the right direction in finding beneficial solutions for the industry as a whole, we believe that some definitions and changes to the standard would benefit from some clarification. Therefore, we suggest the following for the SDT to consider:

AEP had difficulties agreeing with the Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions proposed because they both rely on the proposed Electronic Security Zone (ESZ) definition. AEP found the ESZ definition to be unclear and would benefit from clarification regarding what “systems” and “components” are included in this definition.

Recommendation: AEP recommends that the SDT clarify the new proposed NERC Glossary Terms. AEP also asks SDT to ensure that those who do not plan on implementing virtualization are not affected by these proposed modifications.

Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	

CHPD conditionally agrees with the VCA definition, although not in combination with the proposed SCI definition. The SCI definition currently appears to apply to any virtual system even if that system hosts no CIP-classified systems due to the use of the language “Virtual Cyber Assets **or** that perform logical isolation for an ESZ or ESP”. This appears to create “chicken or egg” scenario when Cyber Assets against the SCI and VCA definitions. CHPD recommends that either the VCA definition be adjusted to scope this classification to more closely resemble the PCA definition or revise the SCI definition to only be applicable when a virtual system is hosting a classified BES Cyber Asset.

Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	

Answer	No
Document Name	

Comment

VCA – agree with proposed definition.

SCI – request clarification on what is meant by “its management systems.”

In the SCI definition - Recommend deleting “or ESP” to confine SCI to virtualized firewalls for ESZs, allowing non-virtualized firewall hardware to be solely classified as EACS and not require dual categorization as both EACS and SCI.

Also recommend retaining the EAP definition (at least within the Glossary of Terms) as a useful and necessary term for management of ESPs, but have no objection to the removal of EAP from R1.2 to accommodate virtualization. Note: If EAP is to be removed, also need to remove the reference in VSL Table under R1 on p. 17.

IRA definition change – this revision to the definition goes beyond what is necessary for a conforming change and what was requested and authorized by the SAR (see Question 8).

The SAR recommends improving clarity within the IRA definition of the phrase “using a routable protocol” with respect to Dial-up Connectivity. This could be addressed by changing the phrase to “using a routable or dial-up protocol.”

We agree with EEI comments that changes to the IRA definition should be limited to modifying the phrase to “using a routable or dial-up protocol.”

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

The Exelon companies agree with the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1,3

Answer	No

Document Name	

Comment

Eversource believes that virtualization is permitted under the current versions of the CIP standards and modification to the existing CIP standards to accommodate the concept of virtualization is not necessary.

Based on the proposed language, Eversource does not support the current definition of the Electronic Security Zone (ESZ) and, therefore, cannot not support the Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions that rely on the ESZ definition. The ESZ definition provided does not clearly identify what an ESZ is or what the terms “systems” or “components” actually mean or would include. We recommend that ESZ definition be revised to clearly identify what those items are and what they would include.

Also, for entities who do not have ESZ in their environment, the current proposal has the potential to create a substantial compliance burden by requiring integration of this concept into their current processes and require these entities to demonstrate they are not utilizing a virtual environment within their networks.

For this reason, Eversource members are concerned that the proposed changes to the base construct of the CIP Standards will prove to be expensive to administer while providing little or no associated reliability and security benefit over the existing CIP language.

Recommendation: Eversource asks the SDT to consider revisiting the current approach that includes new NERC Glossary Terms along with revisions to existing terms and Requirements. We believe virtualization is already permissible within the current language in the existing CIP Standards.

Eversource recommends segregating the proposed changes to the CIP standards into smaller activities, or a more measured incremental approach, to address virtualization. The proposed modifications to CIP-007 R2 and CIP-010 R1 are places where incremental changes could be made without incorporating the ESZ and related virtualization concepts.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

While ISO-NE agrees that the current definitions associated with BES Cyber Systems do not adequately account for virtualization, ISO-NE cautions that adding new terms and definitions continues to foster an object of requirement approach instead of moving towards an information security objective based approach.

It is difficult to ascertain whether the definitions of Virtual Cyber Asset (VCA) and Shared Cyber Information (SCI) are adequate and determine the impact of the new definitions without seeing the revisions in the other standards/requirements, specifically CIP-007 and CIP-010.

To achieve the backwards compatibility, all existing terms must remain in place. In addition, introducing the concept that assets can be have multiple classifications can have profound influence on processes and tools already implemented.

The definition of SCI includes shared storage as one of the functions involved with such systems that requires appropriate protections be considered as part of developing systems and services leveraging virtualized resources. However, the requirements including SCI among Applicable Systems do not then refer to sharing of storage when sharing of CPU or memory is mentioned (CIP-005-7 R1.6, R2.6).

Likes 0	
Dislikes 0	

Response

Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5

Answer	No
Document Name	

Comment

SDG&E supports EEI's comments submitted on our behalf.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar / Kansas City Power & Light support Edison Electric Institute's (EEI) response to Question 1.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI supports SDT efforts that enable registered entities to utilize virtualization within their NERC CIP Cyber Security Networks. While we recognize that a limited number of registered entities have already deployed some form of virtualization within their networks in ways that have been deemed acceptable by their Regional Entities, current auditing and enforcement of such practices is inconsistent across the regions. For this reason, EEI appreciates SDT efforts to listen and respond to industry concerns shared during the previous informal commenting opportunity. EEI's members understand the complex issues the SDT is seeking to address and we appreciate the opportunity to provide feedback on its current proposals.

EEI is of the opinion that the changes provided in this latest proposed approach to virtualization is another good step forward in finding solutions that benefit the Industry broadly. However, additional clarity is still needed. Within this context we offer the following suggestions for SDT consideration:

The currently proposed definition for Electronic Security Zone (ESZ) is not clear. The ESZ definition should address what the terms "systems" or "components" mean or would include. It is difficult to support the Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) definitions currently since they rely on the ESZ definition. In contrast, the non-virtualized and currently approved term Electronic Security Perimeter (ESP) provides clear language that limits an ESP to "networks to which BES Cyber Systems are connected" providing well-defined direction to entities. For this reason, we ask the SDT to revise the proposed definition of ESZ consistent with the approved definition of ESP.

In addition to the concerns identified above, we would like to offer some additional suggestions for SDT consideration:

1. Electronic Access Point (EAP) – EEI recommends that the SDT not propose the retirement of EAP given "ESP's and EAPs remain a valid option and are one method of implementing logical isolation." (see Technical Rationale, Section: Logical Isolation; page 14)

2. Interactive Remote Access (IRA) – EEI recommends that the SDT retain much of the existing text contained within the approved definition for IRA. While we recognize that the SAR directs the SDT to improve the clarity of ESPs, ERCs and IRAs, we are of the opinion that the proposed IRA language may create even more ambiguity. For this reason, we suggest limiting future revisions to the definition of IRA to the following:

User-initiated access by a person employing a remote access client or other remote access technology using a routable **or dial-up** protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and ……

Whether the SDT modifies the existing definition of IRA or develops a revised version of what is currently proposed, efforts should be made by the SDT to ensure that the scope of IRA is clear and doesn't bring in cyber assets not currently covered under this definition.

Recommendation: EEI asks the SDT to clarify the new NERC Glossary Terms along with revisions to existing terms and Requirements and ensure that entities not currently planning to implement virtualization are not impacted by the proposed changes. While virtualization has been permitted within the current language of the CIP Reliability Standards, EEI understands that such practices are not consistently applied by all regions at this time. For this reason, we support the SDT's efforts to develop solutions that make it easier for entities to more fully deploy virtualization as they deem appropriate to achieve internal efficiencies. Additionally, we appreciate efforts by the SDT to ensure that those not seeking to deploy virtualization will not have their existing policies, processes, and procedures upended as a result.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

The term VCA by the definition provided includes current EACM (EAC and EAM) and PACS (PAC and PAM) devices without making a differentiation between them and BCAs and PCAs that are also Virtual. In our opinion, this lack of differentiation of the terms will create ambiguity in the drafting of CIP standards. The currently proposed change to CIP-005 R1.1 would require any virtual PAC or EAC to be included in an ESP or ESZ while Physical PACs and EACs could be located outside that ESP or ESZ.

Additionally the proposed term SCI includes both virtual hypervisor systems as well as traditional firewalls and systems. Technologically speaking those systems are vastly different and will apply to standards in different ways. For example, the proposed change to CIP-005 R2.1 requires that Interactive remote access be limited to an intermediary system for SCI which would be possible for a Hypervisor inside of an ESP but a firewall that creates the boundary of the ESP can't easily have its external interfaces limited down to just the Intermediate system due to its placement in the network.

We propose that SDT modify the definition of "Cyber Asset" to include "Virtual Cyber Assets" instead of establishing another term with essentially no difference of criticality, protection, or evidence within the standard.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

Can the drafting team explain if the intent or expectation of the proposed BES CA definition relative to CIP-002 categorization? Does the team expect 1.) No change? 2.) Decrease in scope by removal of existing BESCA hardware hosting in-scope VCA? Or 3.) Increase in scope by the addition of excluded Cyber Assets that contain “in-scope VCAs”?

The inclusion of both Cyber Asset and Virtual Cyber Asset in the revised definition of BES Cyber Asset could lead to an expansion of Cyber Assets and BES Cyber Assets that are in scope. This could have unintended consequences to the fleet of CIP Standards and could unintentionally cause ambiguity and complexity in tracking procurements of BES Cyber Assets applicable to CIP-013-1 by including “excluded programmable devices” containing “in scope Virtual Cyber Assets”.

Additionally, due to the ambiguity described above, GTC encourages the team to develop a reference document modeled after NERC’s “Bulk Electric System Definition Reference Document” to include various examples containing diagrams of Virtual Cyber Assets and Shared Cyber Infrastructure at each CIP-002 asset location (control center, transmission station and substation, generation resources, etc.) to assist the industry with the application and to provide clarification of the new and revised definition(s) in a consistent, continent-wide basis for the majority of BES Cyber Assets under the proposed definition.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	No

Document Name	

Comment

N&ST disagrees with the proposal to break out monitoring functions from the existing EACMS and PACS definitions in order to serve the goal of easily accommodating third-party, possibly cloud-based, electronic and/or physical access monitoring. We strongly disagree with the rationale that “access monitoring” is somehow less critical, and poses less inherent risk, than “access control,” particularly in light of the fact the 2016 SANS / E-ISAC analysis of the attack on Ukrainian power grid cited a lack of monitoring as a key factor in the attack’s success.

N&ST believes the proposed definition of “ESZ” is inadequate and lacks any intrinsic meaning. We suggest that it be modified by adding words that convey it is a logical boundary, established in a virtual environment, that contains one or more virtual cyber assets and provides logical isolation.

N&ST believes the proposed definition of “SCI” should be modified to reflect the fact that it includes hardware, as per the Technical Rationale document.

N&ST believes the proposed modification of “IRA” has been watered down to the point where it basically defines “Interactive Remote Access” as remote access that’s interactive. While we concur with removing as much “requirements-like” language from Glossary definitions, we believe the revised definition should retain the information that “IRA” is access to a BES Cyber System or associated applicable system and that it is initiated from outside the ESP or ESZ where the system being accessed is located.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

VCA – agree with proposed definition.

SCI – request clarification on what is meant by “its management systems.”

In the SCI definition - Recommend deleting “or ESP” to confine SCI to virtualized firewalls for ESZs, allowing non-virtualized firewall hardware to be solely classified as EACS and not require dual categorization as both EACS and SCI.

Also recommend retaining the EAP definition (at least within the Glossary of Terms) as a useful and necessary term for management of ESPs, but have no objection to the removal of EAP from R1.2 to accommodate virtualization. Note: If EAP is to be removed, also need to remove the reference in VSL Table under R1 on p. 17.

IRA definition change – this revision to the definition goes beyond what is necessary for a conforming change and what was requested and authorized by the SAR (see Question 8).

The SAR recommends improving clarity within the IRA definition of the phrase “using a routable protocol” with respect to Dial-up Connectivity. This could be addressed by changing the phrase to “using a routable or dial-up protocol.”

We agree with EEI comments that changes to the IRA definition should be limited to modifying the phrase to “using a routable or dial-up protocol.”

Likes 0	

Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	Yes
Document Name	

Comment

In general, GSOC/OPC supports the development of new terms and definitions to ensure appropriate clarity regarding the use of virtualization within environments to which CIP is applicable. GSOC/OPC does, however, have concerns regarding clarity around the potential for non-CIP virtual instances being pulled into “scope” by virtue of the expansive nature of the definition of Cyber Asset. In particular, GSOC/OPC is concerned that the inclusion of both Cyber Asset and Virtual Cyber Asset (VCA) in the revised definition of BES Cyber Asset (BCA) could create redundancy and lead to an expansion of the Cyber Assets and BCAs that are in scope. Specifically, the term Cyber Asset has traditionally encompassed hardware and all instances of software thereon. While VCA is applicable only to the logical instances of a Cyber Asset on Shared Cyber Infrastructure (SCI), the inclusion of the term Cyber Asset without additional clarification could be interpreted to pull in the physical infrastructure associated with a VCA and, as a result, all other logical instances running within the virtualized environment. For this reason, GSOC/OPC recommends that the SDT consider adding clarification to the definition of a BCA to ensure that instances of non-CIP virtualized cyber assets that are logically isolated from BCAs or any other applicable system and being maintained on the same hardware as a VCA (without any other interaction) are not pulled into scope of the CIP Reliability Standards.

A Cyber Asset or Virtual Cyber Asset (**excluding Shared Cyber Infrastructure**) that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Note: Virtual Cyber Assets that are logically isolated from and not classified as a BES Cyber Asset are excluded.

Alternatively, if the recommendation for clarification to the definition is not accepted, GSOC/OPC would recommend that the SDT develop compliance and/or implementation guidance concurrently with its standards drafting activities that addresses the need for this clarification. Such effort to develop concurrent compliance and/or implementation guidance was conducted by the SDT to ensure clarity during the development of the BES Definition and was enormously well received by and helpful to the industry during compliance implementation. GSOC/OPC would suggest that any compliance and/or implementation guidance provide diagrams similar to those provided on pages 39 - 40 (Pinecone Energy).

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Please add language to help describe tools such as AV, etc.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Reclamation agrees with the rationale behind adding Virtual Cyber Asset (VCA) and Shared Cyber Infrastructure (SCI) to allow requirements to be specifically targeted at virtualized environments. Reclamation recommends the SDT create a new term for Physical Cyber Assets, and have Cyber Assets be the generic term for both physical and virtual.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
SWG agrees with the concepts of the new definitions. However, there are issues with the definitions.	

SCI: Consider rewording as “storage and its associated network transport.” Provide clarification on how a switch within an ESP or should be classified under this new construct. VCA: The definition does not address “data” consistent with the Cyber Asset definition.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Can the SCI section in the Technical Rationale document have a graphic and description added to address Logical Unit Number (LUN) isolation with respect to Logical Isolation Zones? The document is currently silent on LUN Isolation with respect to satisfying requirements. Additionally, there should be consideration for creating a new term Physical Cyber Assets to support the use of the term or Cyber Assets should be modified to Physical Cyber Assets. Recommend the SDT make considerations for all CIP standards impacted by virtualization be updated concurrently to ensure efforts to make the necessary modifications to existing architecture by the entity.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	

Answer	Yes
Document Name	

Comment

Seattle City Light appreciates the long and hard efforts of the Standards Drafting Team (SDT) in conceiving a way forward for virtualization within the context of the CIP Standards, and for creating extensive supporting materials to explain the proposed concepts and changes. City Light agrees that CIP Standard changes are necessary to support virtualization, and that some new definitions will be required.

However, City Light is concerned about both the expanding number of new definitions and their unique NERC-only nature. Specifically, is the operational function or risk presented by PAMS and EAMS sufficient that they require unique definitions and requirements, or would it reduce risk enough if the data/information contained within them be protected as BCSI (and the terms PAMS and EAMS be dropped entirely)? Could they be considered as another kind of PCA or VCA?

Regarding the proposed change to the PSP definition—"the physical border at which access is controlled"—City Light requests that the SDT clarify what it is the border ***of****. Presumably of something around subject BCS, BCA, VCA hosts, SCI hosts, EACS hosts, etc., but the definition as proposed is in no way clear and promises all kinds of possible audit shenanigans.*

Likes 0	
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

CAISO agrees with the concepts of the new definitions. However, there are issues with the definitions.

SCI: Consider rewording as "storage and its associated network transport." Provide clarification on how a switch within an ESP should be classified under this new construct.

VCA: The definition does not address "data" consistent with the Cyber Asset definition.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally supports the need for the definition of Virtual Cyber Assets and Shared Cyber Infrastructure in the CIP environments.This definition doesn't address the issue of mixed trust environment. It doesn't allow for the existence of non-BES and BES cyber assets (or Virtual Cyber Assets) to exit within the same SCI. SCI is subject to same level of requirement as BCA, and doesn't help entities employing mixed trust environment.

Likes 0	
Dislikes 0	

Response
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	Yes
Document Name	

Comment
MISO agrees with the concepts of the new definitions; however, recommends the following issues be addressed. SCI: Consider rewording as “storage and its associated network transport.” Provide clarification on how a switch within an ESP should be classified under this new construct. VCA: The definition does not address “data” consistent with the Cyber Asset definition.

Likes 0	
Dislikes 0	

Response
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	Yes
Document Name	

Comment
Tri-State recommends the term SCI be changed to “Virtual Infrastructure” and then within the definition add a clarifying statement regarding cloud. Something like: “This infrastructure resides on the Responsible Entity’s premises; not in a 3rd party’s infrastructure.” Additionally, we think the use of “shared” within the definition is problematic, as it carries different meanings and could be interpreted in multiple ways. So, we recommend the team modify this to reflect what we think was intended, which is a mixed or hybrid infrastructure that includes both virtual and physical assets. Everything else about the definition we think is ok, as it relates to the proposed CIP-005. We will need to see how it is applied in the other CIP standards, especially CIP-007 and CIP-010, before we are completely comfortable with the new definition. Tri-State does not agree with the new IRA definitions; see question 8 for additional comments.

Likes 0	
Dislikes 0	

Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
PG&E indicates the following: 1 - Agrees with the proposed new definitions. 2 – Understands the addition of these definitions will allow Entities to use the more advanced features of the technology, while at the same time establishing the conditions within the Requirements to protect the virtualized environments from some their unique vulnerabilities due to the elimination of mixed-trust environments. 3 – Understands the use of these definitions will require modifications to the internal CIP-002 process to document that a BES Cyber System (BCS) can be comprised of more than the current BES Cyber Asset (BCA).	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Patricia Boody - Lakeland Electric - 1,3,5,6

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE disagrees with the explicit exclusion of Shared Cyber Infrastructure (SCI) from the proposed definition of BES Cyber Asset. In the provided rationale document the SDT states that it recognizes that SCI has the same impact as a virtual BCA, or more so if the SCI is hosting multiple virtual BCAs. It appears the SDT acknowledged this by expressing its intention to include SCI in all requirements that currently affect BCA and to include SCI in additional requirements. It also seems it is not consistent with how other categorizations are being applied. The SDT did not include exclusions for

SCI in the definitions of EACS, EAMS, PACS, or PAMS. Additionally, the solution outlined by the SDT requires that all future drafting teams include SCI in the applicable system column for, at a minimum, those requirements applicable to BES Cyber Systems. Other situations also arise. Will SCI that hosts EACS that are associated with Medium/High Impact BES Cyber Systems be included in Applicable Systems? Will Applicable Systems in include SCI hosting PACS that are associated with Medium/High Impact BES Cyber Systems? For example, CIP-007-6 R2 requires that registered entities maintain a security patch management process for applicable systems. Will this requirement be re-scoped to apply to SCI hosting EACS, SCI hosting PACS, etc.? If yes, then this has the potential to make the applicable systems column of certain requirements unnecessarily verbose when including all combinations of BCS, EACS, EAMS, PACS, PCAs, and the SCI hosting all of these. If no, then this has the potential for a compliance gap for SCI that are not hosting BCS but are hosting EACS or PACS. For example, if CIP-007-6 R2 is not written to apply to "SCI hosting EACS associated with High or Medium Impact BES Cyber Systems" then the SCI may receive less protection then the VCAs it hosts. Alternatively, if the expectation is that SCI hosting PACS are categorized as PACS and SCI hosting EACS are categorized as EACS then the categorization of SCI hosting BCS will not follow the same logic. Instead, Texas RE recommends that applying multiple categorizations to Cyber Assets that perform multiple functions is the easiest solution to this issue. Currently if an entity has an EACMS and places it inside an ESP, it is expected to comply with EACMS and PCA requirements. SCI should be treated in the same manner. If a Cyber Asset is performing the function of an SCI then it should be categorized as an SCI and inherit all of the categorizations of the VCAs it hosts.	
Likes 0	
Dislikes 0	
Response	

2. The CIP SDT tried to maintain backwards compatibility throughout CIP-005. However, in order to take advantage of emergent technologies the existing firewall that were associated with an EAP will now fall into the SCI definition and be subject to CIP-005 Requirement R1 Part 1.6, which requires management plane separation. What level of effort would be required to accommodate these changes? Do you agree? If not, please provide comments to support your response. (CIP-005 Technical Rationale pages 11, 13, and 29-32).

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant supports MRO NSRF's comments.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

We disagree with the premise of the question. Per CIP-005 R1.6 it applies to only SCI hosting HIBCS and MIBCS. If the EAP is on SCI that does not host HIBCS or MIBCS then management plane separation is not required. If that we the intent, then the proposed requirement failed to achieve the objective. Also, per our response in comment #3 the SCI definition needs to have the third bullet struck due to the infinite recursion of CIP-005 R1.1.

The purpose of the proposed CIP-005 is “To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication.” Controlling access to the management plane of a device that isn’t a BES Cyber System appears to be outside the purpose of the standard, thus EACS performing logical isolation should not have their management plane in scope.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Please see the comments to Question 1. Southern does not agree that all EACS should be dual classified as SCI as well; some should, some should not. The level of effort required to accommodate these changes could be significant, but could be lessened by consideration of proposed changes provided in our responses to previous questions.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Based on our comments in the question 1, SCI is not needed since it would fall within the definition of BCS, EACMS or PACS. Therefore CIP-005 R1 Part 1.6 applicable system should be changed to high and medium BCS and associated EACMS and PACS.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

This is not only an addition to CIP-005, but also CIP-007 and CIP-010.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

There is no need to sacrifice backwards compatibility by incorporating the existing firewalls (EAPs) associated with ESPs into the SCI definition.

A “next gen” firewall with virtualized firewalls can be designated SCI per the definition (although the device could also meet the definition of EACS, complicating categorization and compliance tracking). If “or ESP” is deleted from the SCI definition, then hardware firewalls associated with ESPs can be EACS and not be subject to SCI applicability, maintaining backwards compatibility.

If a firewall is not virtualized, there is nothing to do per R1.6; it doesn’t apply, so also delete “or ESP” from the Requirements of R1.6.

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

We believe the combination of Virtual infrastructure and traditional firewalls and switches into a single definition will be confusing in the drafting of CIP standards. Both systems provide drastically different functions and will be located in two distinct parts of the network. Due to the placement of a firewall system at the edge of an ESP/ESZ a great deal of extra effort would need to happen to create a new interface and ESP for a new management plane.

Likes 0

Dislikes 0

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

See EEI's response to Question 1

Likes 0

Dislikes 0

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 2.	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
As already mentioned above, to achieve the backwards compatibility, all existing terms must remain in place. In addition, introducing the concept that assets can be have multiple classifications can have profound influence on processes and tools already implemented.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	

Comment

See Eversource response to Question 1

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

PPL NERC Registered Affiliates appreciate the SDT's effort to make the updated requirements backwards compatible. We agree that in a mixed-mode virtual environment, isolation between the management plane and data plane is imperative (with mixed-mode meaning, for example, high/medium BES Cyber Systems, BES Cyber Systems/EACS, or CIP/non-CIP). However, if an entity sets up separate virtual environments (i.e. a high impact BES Cyber System virtual environment and a separate associated High Impact EACS environment), we believe that isolation between the management plane and the data plane will require a significant amount of additional work (i.e. design changes on every existing firewall) resulting in elevated compliance risk and zero benefit. The SDT should continue to consider that not all virtual environments that involve CIP will be mixed-mode.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

The Exelon companies agree with the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No

Document Name	
Comment	
AZPS warns against retiring the EAP definition. If the ESP definition will be maintained the EAP definition should follow. This modification would force changes throughout the categorization process AZPS has in place and does not allow for the specific requirements to be applied to a virtual vs. physical firewall. Further, requirement part 1.6 does not include instruction on how to address a physical EAP with a nonexistent separate management plane.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
There is no need to sacrifice backwards compatibility by incorporating the existing firewalls (EAPs) associated with ESPs into the SCI definition. A “next gen” firewall with virtualized firewalls can be designated SCI per the definition (although the device could also meet the definition of EACS, complicating categorization and compliance tracking). If “or ESP” is deleted from the SCI definition, then hardware firewalls associated with ESPs can be EACS and not be subject to SCI applicability, maintaining backwards compatibility. If a firewall is not virtualized, there is nothing to do per R1.6; it doesn’t apply, so also delete “or ESP” from the Requirements of R1.6.	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
CHPD cannot ascertain how to achieve compliance with the proposed language. CHPD requests a definition for “Management System” and “Management Plane”. CHPD also requests clarification on the inclusion of CPU and memory and how those terms are applied to this requirement. Please include a real-world example of successful compliance with this language.	
Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
The Technical Rationale explains that the purpose of this requirement is to require isolation between the data and management planes, therefore the requirement should directly state that to be clear on its intent. Also, the word “may” should be replaced with “can” to be more definite and provide better clarity. CenterPoint Energy Houston Electric, LLC (CenterPoint Energy) recommends the following language: “Management systems must be logically isolated from the data plane and can only share CPU, memory or ESZ or ESP with other management systems and the management plane.”	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	
Please see AEP’s response to Question #1	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	No
Document Name	
Comment	
There is no need to sacrifice backwards compatibility by incorporating firewalls associated with ESPs into the SCI definition. A “next gen” firewall with virtualized firewalls can be designated SCI per the definition (although the device could also meet the definition of EACS, complicating categorization and compliance tracking). If “or ESP” is deleted from the SCI definition, then hardware firewalls associated with ESPs can be EACS and not be subject to SCI applicability, maintaining backwards compatibility. If a firewall is not virtualized, there is nothing to do per R1.6; it doesn’t apply, so also delete “or ESP” from the Requirements of R1.6.	

Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
There is no need to sacrifice backwards compatibility by incorporating firewalls associated with ESPs into the SCI definition. A “next gen” firewall with virtualized firewalls can be designated SCI per the definition (although the device could also meet the definition of EACS, complicating categorization and compliance tracking). If “or ESP” is deleted from the SCI definition, then hardware firewalls associated with ESPs can be EACS and not be subject to SCI applicability, maintaining backwards compatibility. If a firewall is not virtualized, there is nothing to do per R1.6; it doesn’t apply, so also delete “or ESP” from the Requirements of R1.6.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	

See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT agrees with the concept. The level of effort for implementation will be dependent on how entities have already architected systems.	
Likes 0	

Dislikes 0

Response

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC

Answer	Yes
Document Name	

Comment

For the two (2) part question, PG&E indicates:

1 – The effort to accommodate the indicated changes will be minimal. PG&E currently approaches the separation of the management plane in a manner that is similar to what is shown in the proposed Requirement part 1.6.

2 – PG&E agrees with the proposed modification on the separation of the management plane from other Cyber Asset types (i.e. BCS), but has a concern that the phrase “may only share CPU, memory, or ESZ or ESP with other management systems and the management plane” indicates the same condition being presented in Questions 4 and 5, which may not be clear to many. Questions 4 and 5 indicate PCA (virtual type) or BCS of different impact ratings must take on the impact rating of the highest impact-rated Cyber Asset in the same ESZ, ESP, or sharing the same CPU and memory (i.e. no mixed-trust). PG&E believes this condition extends to SCI, but that is not made clear by the mixed-trust section of the currently-drafted Technical Rationale document.

Recommendation - If PG&E’s understanding is correct and SCI of different impact ratings cannot share the same CPU and memory (i.e. no mixed-trust), PG&E recommends the Technical Rationale section on mixed-trust be modified to clearly indicate SCI of different impact ratings cannot share the same CPU and memory.

Likes 0

Dislikes 0

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	Yes
Document Name	CIP 005_Q2 Diagram.pdf

Comment

Based on the current draft, it appears we would have to purchase multiple pieces of physical hardware to create a management plane separate from the SCI. The level of effort depends on how the auditors approach/define management systems, management plane and data plane. We feel the SDT should define management systems, management plane, data plane, and give examples for all three terms. Here are some suggested definitions for each:

In this scenario the Hypervisor is classified as a BCA based on the high water mark. Let’s assume to access the hypervisor an administrator authenticates to the hypervisor through a web interface hosted on the hypervisor. The web connection is initiated from a workstation (BCA) from inside the ESP. All traffic between VLANs run through a switch to the firewall, for logical isolation. In this example, the hypervisor will share the same CPU and memory as the data plane, therefore would not be compliant with CIP-005 R1.6. So would the hypervisor or workstation be considered a management system in this situation? The standards should allow for this type of configuration when there is no typical “management system” used to administer multiple VM infrastructures.

- Management system – a device used to remotely manage a VM infrastructure. This is a separate device that does not share CPU or memory with the VM infrastructure. This does not include the local hypervisor embedded management interface.
- Management plane – a collection of management systems used to remotely manage VM infrastructures. This is a separate collection of devices that do not share CPU or memory with the VM infrastructure. This does not include the local hypervisor embedded management interface.
- Data plane – shared storage system used by more than one SCI (does not include the hypervisor local storage)

We agree with this approach if the entity is using a separate, central “management system” to administer multiple virtual infrastructures (virtual farm). However, based on the wording of CIP-005 R1.6, it does not allow for a single virtual infrastructure inside the ESP to be managed locally by directly logging into the hypervisor. An entity would need additional physical equipment in order to manage the hypervisor and be compliant with CIP-005 R1.6. Any hypervisor would essentially share resources such as CPU, Memory and Disk with its locally managed VMs.

We have a scenario we would like to see addressed in the standard changes; see uploaded diagram in addition to the following comments:

In this scenario the Hypervisor is classified as a BCA based on the high water mark. Let’s assume to access the hypervisor an administrator authenticates to the hypervisor through a web interface hosted on the hypervisor. The web connection is initiated from a workstation (BCA) from inside the ESP. All traffic between VLANs run through a switch to the firewall, for logical isolation. In this example, the hypervisor will share the same CPU and memory as the data plane, therefore would not be compliant with CIP-005 R1.6. So would the hypervisor or workstation be considered a management system in this situation? The standards should allow for this type of configuration when there is no typical “management system” used to administer multiple VM infrastructures.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	Yes
Document Name	

Comment

MISO agrees with the concept. The level of effort for implementation will be dependent on how entities have already architected systems. Worth noting, this particular subpart is somewhat prescriptive and will be wholly new. Many entities may have difficulty complying if the timeline for compliance is short; i.e. less than 3 years. MISO is recommending a 3-year timeline for implementation as, depending upon when the standard is approved, an entity will need to identify the additional equipment needed, plan for the anticipated expense duing its next budget cycle, order the equipment once the budget is approved and test and install the equipment upon delivery.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Changes to eliminate to defined term EAP will require a moderate level of effort for a small entity with limited number of EAP devices. For a larger entity, the level of effort could be significant. It will require changes to policies, procedures, network diagrams, and possibly other evidence artifacts to incorporate the new defined terms and remove the old ones.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the direction of backwards compatibility and is currently assessing the impact of the SCI definition requiring management plane separation	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO agrees with the concept. The level of effort for implementation will be dependent on how entities have already architected systems. Worth noting, this particular subpart is somewhat prescriptive and will be wholly new. Many entities may have difficulty complying if the timeline for compliance is short.	
Likes 0	
Dislikes 0	
Response	

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light judges that the level of effort required to configure and maintain the required Shared Cyber Infrastructure (SCI) management plane separation is not burdensome given the operational benefits provided by the SCI concept. *City Light also asks that the SDT clarify if an accessing device for a Management Plane (out of band network) can be virtual, or must it be completely separate from the VCA or SCI?*	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Answer assumes that software defined firewalls are in scope of the question. The level of effort is considered low for new implementation. For existing implementations, the level effort can be high depending on the existing architecture. Will Entities be provided a phased in consideration for existing architecture and the implantation guidelines be reflective of the phased in approach?	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
While not a significant level of effort will be required to technically accommodate R1 Part 1.6, this will require a change in culture which introduces compliance risk. This will require Entities to train EAP administrators on the new requirement and modify CIP-010 Change Management process(es) for EAP/LIZ/ESZ. For Entities not moving forward with emergent technologies, this will force programmatic changes to maintain backwards compatibility.	

Further, we have spoken with various major Distributed Control System, SCADA, and Industrial Control System vendors and none of them have customers asking for policy based controls and thus do not have plans in the next 24 months to develop and or integrate them into their products.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
For BPA, the effort will consist of drawing and documentation updates.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
SWG agrees with the concept. The level of effort for implementation will be dependent on how entities have already architected systems. Worth noting, this particular subpart is somewhat prescriptive and will be wholly new. Many entities may have difficulty complying if the timeline for compliance is short.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	

Reclamation sees minimal impact to current and future operations. Reclamation follows FISMA and NIST guidelines in addition to NERC Standards.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees that management plane separation should be required. However, Texas RE seeks clarification in Part 1.6 which states, “Management systems may only share CPU, memory, or ESZ or ESP with other management systems and the management plane.” Does this mean an entity can have SCI that contains corporate **and** CIP management systems/plane, which can share CPU, memory, or ESZ or ESP; thus creating a potential mixed trust virtual environment? This appears to be supported by the CIP-005 Technical Rationale on pages 14-15. Although, mixed trust risks are identified and two option examples are given mixed trust is allowed which is concerning when one could have SCI that includes BCAs: EMS, SCADA, etc. Additionally, based on the proposed BCA definition; SCI is excluded from the BCA definition.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource	

Answer	
Document Name	
Comment	
Recommend changing the proprietary term “hypervisor” with a generic term like “VM host” Request clarification of the diagrams on pages 30-32. Legends explaining the color coding and dotted lines will help. We are not sure about the unmarked boundaries. At least one diagram includes a physical box yet this topic is virtualization . . . thereby confusing what is physical vs what is virtualization Some of us have Part 1.7 on page 32 while others have Part 1.6. Yet both versions are August 2019. Suggest posting once or if updating please broadcast an announcement of new versions. GENERAL COMMENT - this technology is complex which will require a lot of training beyond today’s training. Expecting to re-write documentation too.	
Likes 0	
Dislikes 0	
Response	

3. The SDT is proposing the new term Electronic Security Zone (ESZ) to enable future technologies such as policy based environments. Do you agree with the proposed definition? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. Note: ESP will be retained for backwards compatibility. (CIP-005 Technical Rationale pages 10, 14-18, 22-26, and 38-40).

- **Electronic Security Zone (ESZ): A segmented section of a network that contains systems and components to create logical isolation.**

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	No
Document Name	

Comment

GSOC/OPC respectfully suggests that the definition be revised for greater consistency with the definition of an Electronic Security Perimeter (ESP) as follows:

ESZ: A logically isolated section of a network that contains BES Cyber Asset(s), Electronic Access Control System(s), Electronic Access Monitoring System(s), Physical Access Control System(s), Physical Access Monitoring System(s), Protected Cyber Asset(s) or their management components.

Further, even in this revised definition, it is unclear how this definition would apply for policy based environments when the policy is applied to workloads and not network segments. It appears that while the issue of whether the policy has to apply at layer 3 in the OSI model is addressed, the effect is that it is still only permissible for the policy to apply to the network - instead of other elements of the system that may effectively control access.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

Current definition could lead to the inclusion on VLANs that are used for performance and not necessarily security.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

We disagree with ESZ definition. Given that SCI is not needed for addressing the virtualization (See our rationale in question 1), the ESZ is not needed either. The following are the rational for not defining the ESZ:

- If the ESZ is for the defense in depth and adds network layer access control for further protecting EACMS and PACS (the current requirements don’t require zone protection for EACMS and PACS), we suggest modifying the existing ESP to address this as follows:

“The logical bonder surrounding a network to which BES Cyber Systems, EACMS and PACS are connected through using routable protocol.”

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT agrees with the concept and offers the following modification for your consideration: “One or more segmented sections of a network used to create logical isolation.”

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern asks the SDT to consider the following changes to the Electronic Security Zone definition:

Electronic Security Zone (ESZ): A segmented logical boundary used to protect Virtual Cyber Asset applicable systems using logical isolation.

This proposed change attempts to clarify the use of ESZs as being in virtual space, allowing for backward compatibility and continued use of traditional ESP/EAP configurations for those choosing not to apply virtualized concepts. Additionally, we recommend removing the words “of a network” as this is in conflict with the overall virtualization concepts.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
We agree with the definition of ESZ, but ESP needs to be revised or retired. The definition of Electronic Security Zone does not have a qualifier to restrict scope to BES Cyber Systems like its sister term, ESP. Furthermore CIP-005 R1.1 has been expanded to include PACS and EACS hosted on SCI. If those PACS and EACS are not on the same network as a BCS then by definition they are not within an ESP and an entity must place them in the ESZ since no such qualifier currently exists. There are other issues, but they relate to the requirement and are addressed in comment #9. It would seem that ESP could be retired and replaced with just the ESZ term as written. We have not thought of a case where the term ESZ term could not be used in place of ESP. This would still keep backwards compatibility as older ESPs just now be an ESZ. In addition, PSP was revised with its qualifying language removed indicating it will be moved to CIP-006 requirement. This is another reason to provide conformity and replace ESP with ESZ.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
Consider using ESZ or ESP and elaborating on the definition of the one used.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No

Document Name	
Comment	
SWG agrees with the concept. We offer a modification for your consideration, “One or more segmented sections of a network used to create logical isolation.”	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels. See Question 5	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	No

Document Name	
Comment	
We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels. See Question 5.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	
Please see AEP’s response to Question #1	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
The definition is unclear, technically and in its literal meaning. A zone is not a network or a segmented section of a network. A zone does not contain only the systems or components that create logical isolation, but also includes the systems or components being isolated. CenterPoint Energy recommends the following definition for the term Electronic Security Zone: “Systems or components that create policy-based logical isolation to control access to and/or from applicable Cyber Systems, applications, or data whether singly or by group.”	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource	
Answer	No
Document Name	
Comment	

Comments on the Definition

We recommend changing from “A segmented section of a network that contains systems and components to create a logical isolation” to “is a network that is logically isolated” because the network is logically isolated, a segment is not. The network does not “contain systems and components to create a logical isolation.”

Likes 0	
Dislikes 0	
Response	

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels. See Question 5.

Likes 0	
Dislikes 0	
Response	

Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	

The Exelon companies agree with the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	
Comment	
See Eversource response to Question 1	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO agrees with the concept. We offer a modification for your consideration, “One or more segmented sections of a network used to create logical isolation.”	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Comments: The term “segmented” should be clarified regarding the properties of a given network that would be used to identify systems in or out of a given “segment” (generally, layer 1, layer 2, and/or layer 3 would make sense). This could mean IP Address-based segmentation (i.e. layer 3), or MAC address based list of specific network interfaces (or vlans) (i.e. layer 2), or use of specific sets of cables (i.e. layer 1). It would also help to better define the concept of “isolation” with respect to member systems in a “segment.” Does “isolation” in this case specify limiting network traffic altogether between member systems or only between member systems and non-member systems or something else entirely? Or can isolation involve only partial restriction of network traffic (i.e. white/black lists of ports or protocols or even particular attributes of application use of a protocol)? It would be much more clear to identify what characteristics of communication are expected to be addressed with “isolation.” If the intended	

effect is to cut off all network communication between isolated and non-isolated systems, this might be better described as network isolation or communication isolation. Another approach to addressing the term “logical isolation” might be to clearly call out the parameters associated with “logical” (e.g. addresses, cyber asset make, cyber asset model, connected vlan, http post request headers, etc.). Since particular parameter choices might be considered prescriptive in terms of technology, it may be better to address the goals involved with “logical isolation.” There should be a statement that explains the goal of the “logical isolation” (i.e. whether it is supposed assist with audit, security, or service definition goals related to identifying sets of systems included in “isolation” groups.	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 3.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	

Comment
See EEI's response to Question 1

Likes 0	
Dislikes 0	

Response
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	No
Document Name	

Comment
MISO agrees with the concept. We offer a modification for your consideration, “One or more segmented sections of a network used to create logical isolation.”

Likes 0	
Dislikes 0	

Response
David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment
We believe the term Logical Isolation is unclear and open to misinterpretation by auditors. We request the SDT to include a definition of Logical Isolation or the information in the Technical Rationale in a guidance document to remove any confusion. Without it, some serial devices may be inadvertently pulled into scope for requirements that they do not pertain to.

Likes 0	
Dislikes 0	

Response
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	

Comment

Tri-State agrees with the proposed definition.

Likes 0

Dislikes 0

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC respectfully suggests that the definition be revised for greater consistency with the definition of an ESP as follows:

ESZ: A logically isolated section of a network that contains BES Cyber Asset(s), Electronic Access Control System(s), Electronic Access Monitoring System(s), Physical Access Control System(s), Physical Access Monitoring System(s), Protected Cyber Asset(s) or their management components.

Further, even in this revised definition, it is unclear how this definition would apply for policy based environments when the policy is applied to workloads and not network segments. It appears that while the issue of whether the policy has to apply at layer 3 in the OSI model is addressed, the effect is that it is still only permissible for the policy to apply to the network - instead of other elements of the system that may effectively control access.

Likes 0

Dislikes 0

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	No
Document Name	

Comment

N&ST believes the proposed definition of “ESZ” is inadequate and lacks any intrinsic meaning. We suggest that it be modified by adding words that convey it is a logical boundary, established in a virtual environment, that contains one or more virtual cyber assets and provides logical isolation.

Likes 0

Dislikes 0

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We agree with EEI's comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels. See Question 5.	
Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Reclamation recommends replacing “zone” with “enclave”. Electronic Security Enclave (ESE) – A segmented section of a network that contains systems and components to create logical isolation.	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
While this opens the standards to future technologies, each vendor's approach to policy based environments will be different and will change with technology advances. This will bring auditing challenges for auditors as each vendor will have differing approaches to policy based environments, policy outputs, and ways to present policy versus existing environments with firewalls which can be presented uniformly. We feel prior to approval(s) a standardized approved audit approach should be published for auditing policy based environments.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
The ESZ provides additional flexibility.	
Likes 0	
Dislikes 0	
Response	

Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the added request of including the term VLAN to reduce misinterpretation.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light suggests that the measures for CIP-005-7 R1.2 (and perhaps others) include examples of how the new requirement is met by ESP/EAP concepts, in addition to how the new concepts are applied. To ensure backwards compatibility, it should be clear in the measure provided for these requirements how the SDT envisions that both the old and new approaches can be applied to demonstrate compliance.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the direction of backwards compatibility and the definition of ESZ.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Changes to incorporate the defined term ESZ will require a moderate level of effort for a small entity with limited number of SCI devices. For a larger entity, the level of effort could be significant. It will require changes to policies, procedures, network diagrams, and possibly other evidence artifacts to incorporate the new defined terms and distinguish where the old terms are still being used.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the proposed definition of ESZ since it is the virtual equivalent of ESP. PG&E does have the concern that the addition of this definition will result in additional administrative effort related to documentation of the ESZ since it is possible an ESZ can be created for each virtual Cyber Asset (i.e. micro-segmentation). **Recommendation** - PG&E recommends the SDT get input from the industry on the potential burden and administrative impact, in order to fully understand future documentation effort.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. The SDT is addressing the risk of systems of different impact, trust, or security levels ("mixed trust") environments that are possible on Shared Cyber Infrastructure by modifying the definition of Protected Cyber Asset (PCA) so that it includes those VCA's that can share a hypervisor's CPU or memory. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 8, and 14-15).

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

It is unclear what risks the SDT is trying to address. The rationale mentions the risk of side channel attacks in pages 14-15. However it isn't clear in the standard that is the risk being addressed. The purpose of the proposed CIP-005 is "To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication." Per the purpose we should protect BES Cyber Systems communications and side channel could be considered a form of communication. However it isn't clear why PACS and EACS hosted on SCI are included throughout the standard since protecting their communication is not the purpose of the standard. The page 36 of rationale indicates it is because of the mixed trust issues when they utilize the same SCI. A PACS or EACS utilizing the same SCI as a BES Cyber Asset is by proposed definition a PCA. If the PACS or EACS is virtualized and on the same SCI then bullet #3 of PCA applies. If the PACS or EACS are physical yet are within the same ESZ as the BES Cyber Asset then it could be argued per current proposed definition they are sharing SCI that performs logical isolation of an ESZ or ESP. It is a fallacy of industry that an EACS and PACS cannot be a PCA. By proposed definition if they reside within the same ESP, same ESZ, or share computing resources then they are also a PCA. If the intent is to prevent side channel attacks from EACS or PACS sharing SCI with BCAs then strike PACS hosted on SCI and EACS hosted on SCI from the Applicable Systems as they are already covered by the term PCA. If the intent is to prevent side channel attacks on EACS and PACS then the purpose of the standard needs to be revised and consider controlling communication to all EACS and PACS both physical and virtual. As it stands right now the requirements rope in any EACS or PACS that is virtualized and not just the ones that are on the same SCI as BCAs. The definition of SCI does not restrict to only those devices shared with BCAs. When one looks at the CIP-005 purpose and the rationale it appears expansion of scope to virtualized EACS and PACS is beyond what was intended.

Also, the risk of shared storage is not addressed, but it isn't a communication issue so this could be a CIP-007 item. A VCA could theoretically use up all the remaining storage on the storage array if it was allowed to grow as needed. This could result in a DoS of additional storage needed by a BCA on the same SCI. The problem is not sharing of CPU, memory, or storage. The problem is if there are no policies policing the use of CPU, memory, or storage. Proper policies would mitigate the risk just as well as physically separate hardware.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Based on our comments in the question 1, given that SCI would fall within the definition of BCS, EACMS or PACS, the mixed trust environment cannot be used, where the hypervisor or management plane for hosting or managing the CIP Cyber Assets has to be separated from those that are not used for hosting or managing non-CIP cyber assets.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

The definition groups too many categories together. For example, there may be specific software for the hypervisor. That is not the same as an out of scope VM.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	

Comment

We think more work is needed to future-proof the definition. Would like the definition to be less prescriptive and more qualitative. Would like modifications at a higher level, so we are not limited to today’s environment and explanations. For example, imagine a scenario where multiple VMs with different CIP classifications are hosted on a single hypervisor. Each VM is connected on a separate VLAN to a single virtual managed switch. The virtual switch is connected to a physical switch through a trunked port that carries all the VLANs. The physical switch is physically connected to a firewall, which provides routing and logical separation with ACL.

In this scenario, is there sufficient logical segregation so that we could have an EACMS VM, Out of Scope VM on the same SCI with the hypervisor declared as an EACMS?

Likes 0	
Dislikes 0	

Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI does not support the SDT’s current approach to mixed trust environments. Our primary concern centers on the hypervisor, which is known to have vulnerabilities to cyber-attack through any of the Virtual Cyber Assets (VCA) on the hypervisor. It is our view that securing the VCAs in a lower risk environment at a lower cyber security posture versus the VCAs in the higher risk environment increases the hypervisor’s vulnerability to attack diminishing the protections already established under the CIP Standards. We are also concerned that the proposed definition of PCAs may introduce similar risks, given the linkage between the two terms (i.e., VCAs and PCAs). It is our recommendation that the hypervisor and the control(s) it enables, logical separation of VCAs, need to be considered just as vulnerable as any computer system, whether connected to BES Cyber Systems or not.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 4.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy does not support the modified definition of PCA as currently proposed.This definition does not adequately address the issue of mixed trust environment nor does it allow for the existence of non-BES and BES cyber assets (or Virtual Cyber Assets) to exit within the same SCI. SCI is subject to same level of requirement as BCA, and doesn't help entities employing mixed trust environment.	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
Comments: If the definition of shared attributes (CPU, memory) is to be consistent with the SCI definition, please include in the PCA definition VCAs that share storage with a hypervisor as well.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	
Comment	

Eversource does not support the SDT’s current approach to mixed trust environments. Our primary concern centers on the hypervisor, which is known to have vulnerabilities to cyber-attack through any of the Virtual Cyber Assets (VCA) on the hypervisor. It is our view that securing the VCAs in a lower risk environment at a lower cyber security posture versus the VCAs in the higher risk environment increases the hypervisor’s vulnerability to attack diminishing the protections already established under the CIP Standards.

It is our recommendation that the hypervisor and the control(s) it enables, logical separation of VCAs, need to be considered just as vulnerable as any computer system, whether connected to BES Cyber Systems or not.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

The Exelon companies agree with the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource

Answer	No
Document Name	

Comment

Request confirmation that the intent of new, third bullet in the PCA definition is “Other tenants that share the same host VM as a BES Cyber System become an associated PCA”

Request clarification on this “mixed trust.” Does high watermarking apply in a mixed trust situation?

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	
Comment	
CHPD believes that this is an improvement from the prior definition; however, the inclusion of the third bullet “Share compute resources (CPU or memory) with a BES Cyber System” eliminates the benefits of sharing virtual infrastructure between CIP and non-CIP devices (all non-CIP virtual systems hosted on the same SCI will become PCAs under this language). CHPD proposes that the third bullet be removed.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
The proposed requirement prevents or severely limits use of cloud-based systems. While the risk of virtual machine escape is not zero, it is very small and mitigation through hypervisor patching, integrity checking, or other means is more appropriate than bringing all other hosted tenants into scope. Isolation from other tenants may be impossible on cloud-based systems today, and future industry hosted systems as virtualized environments become the normal way or even required or the only option. The SDT must consider an acceptable way to mitigate virtual machine escape risk that is independent of other tenants.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP does not currently support mixed trust environments, as we believe that hypervisor needs to be considered equally vulnerable as any system regardless of its connectivity to BES Cyber Systems. AEP is of the opinion that the SDT’s current approach makes the hypervisor more vulnerable to attack, negatively affecting the protections already in place as a result of the CIP standards.	
Likes 0	
Dislikes 0	

Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Items separated in the different ESZs should not be categorized as PCAs in order to make the new requirements feasible for implementation. Implementation of Virtual Environments requires the replacement of a certain number of cyber assets to be economically viable. Entities whose physical ESP devices do not themselves reach this threshold will have additional compliance burden and cost from changes to this standard since they will not choose the greater cost to use CIP Virtual Environments due to separate ESZ devices now coming into PCA scope.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	

Answer	Yes
Document Name	
Comment	
Regarding the definition of PCA, please provide an example of a PCA that would be on an ESP. On bullet 2, ERCOT suggests replacing "that" with "and."	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
GSOC/OPC agrees with the intent. However, as discussed above, the inclusion of both Cyber Asset and VCA in the revised definitions of BCA and Protected Cyber Asset (PCA) could create redundancy, lead to an expansion of the Cyber Assets and BCAs that are in scope, and could unintentionally cause ambiguity. For example, the inclusion of a provision around "shared compute resources" seems at odds with the concept of logical isolation proposed and appears to result in a clear expansion of "in scope" cyber assets. For this reason, the proposed definitions could have unintended consequences to the fleet of CIP Standards including CIP-013-1, e.g., the structure of the definitions could result in the inclusion of "excluded programmable devices." As discussed above, revisions and/or clarification to the structure of the definitions is requested to ensure that those VCAs intended to be excluded by virtue of logical isolation are, in fact, excluded and are not inadvertently brought into scope. Alternatively, clarification and guidance could be provided through the development of compliance and/or implementation guidance, similar to the effort that the SDT team undertook when drafting the BES Definition. Such guidance issued should include appropriate diagrams such as those provided on pages 39 – 40 of the Technical Rationale document.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
We agree with the modifications to the PCA definition to incorporate VCAs and shared resources, but do not believe this is sufficient to permit mixed trust, as addressed in Question 5.	

Likes 0	
Dislikes 0	
Response	
Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
We agree with the intent. However, as discussed above, the inclusion of both Cyber Asset and Virtual Cyber Asset in the revised definitions of BES Cyber Asset and Protected Cyber Asset could create redundancy, lead to an expansion of the Cyber Assets and BES Cyber Assets that are in scope, and could unintentionally cause ambiguity. For example, the inclusion of a provision around “shared compute resources” seems at odds with the concept of logical isolation proposed and appears to result in a clear expansion of “in scope” cyber assets. For this reason, the proposed definitions could have unintended consequences to the fleet of CIP Standards including CIP-013-1, e.g., the structure of the definitions could result in the inclusion of “excluded programmable devices.” As discussed above, revisions and/or clarification to the structure of the definitions is requested to ensure that those Virtual Cyber Assets intended to be excluded by virtue of logical isolation are, in fact, excluded and are not inadvertently brought into scope. Alternatively, clarification and guidance could be provided through the development of compliance and/or implementation guidance, similar to the effort that the SDT team undertook when drafting the BES Definition. Such guidance issued should include appropriate diagrams such as those provided on pages 39 – 40 of the Technical Rationale document.	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
This will require discrete zones/networks (CIP management ESZs or ESPs) for ERC to hypervisors as the hypervisor will be considered an associated PCA of the highest impact rating of a guest OS that the hypervisor maintains.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes

Document Name	
Comment	
PG&E agrees with the modification of PCA to include VCA's. This clearly indicates that a PCA can be the current "physical" type of device or the newer "virtual" type of device.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	Yes
Document Name	
Comment	
Regarding the definition of PCA, please provide an example of a PCA that would be "on an ESP." On bullet 2, replace "that" with "and."	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
Regarding the definition of PCA, please provide an example of a PCA that would be on an ESP. On bullet 2, replace "that" with "and".	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

City Light agrees with the concept to high watermark a mixed trust environment, but we find the proposed modifications to the PCA definition can be confusing. Please provide additional clarification.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Is it technology capable to prioritize one VM/VCA over another from a reservation perspective? Not sure how this functionality is involved with respect to ensuring that a ‘mixed trust’ event will not occur. If it is involved, can additional information in the Guidance document be provided?	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
We agree with the modifications to the PCA definition to incorporate VCAs and shared resources, but do not believe this is sufficient to permit mixed trust, as addressed in Question 5.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

BPA believes that mixed trust is not the correct term for shared infrastructure that implements security controls between the differing security zones. Modern technology starts with a zero trust model and then adds necessary, controlled levels of trust through a whitelisting or additive model and therefore controls the risk. The benefit of shared infrastructure includes lower cost of ownership, but also focuses cyber security efforts on what is important rather than spreading scarce personnel or fiscal resources thin for minimal return on effort.

"Mixed trust" as used in other industry and best practices guidance typically means that assets subject to different levels of security control have no security mechanism between them. This is not the case in a properly configured virtual environment.

BPA also believes that there needs to be clear understanding around the difference between “impact level” and “Risk level” as impact is simply one aspect of overall risk, which includes probability, threat actors, vulnerabilities, etc.

Likes 0	
Dislikes 0	

Response

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO

Answer	Yes
Document Name	

Comment

Agree with the modifications to the PCA definition to incorporate VCAs and shared resources, but do not believe this is sufficient to permit mixed trust, as addressed in Question 5.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

Agree with the modifications to the PCA definition to incorporate VCAs and shared resources, but do not believe this is sufficient to permit mixed trust, as addressed in Question 5.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Regarding the definition of PCA, please provide an example of a PCA that would be on an ESP. On bullet 2, replace “that” with “and”.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Consider that quality of service configuration can be applied to overcome mixed trust issues. You can have virtualization workloads with PCA and non PCA environments while guaranteeing compute resources to PCA environments.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE seeks the following clarification on the Protected Cyber Asset (PCA) definition:

- Regarding the statement “*or on an Electronic Security Perimeter*”, what does this mean logically from a networking perspective when A PCA IP address is within an ESP? ESPs are usually IP addresses (ranges, subnets, vlans, etc.).

Likes 0	
Dislikes 0	
Response	

5. The SDT proposes to address infrastructure that is shared between differing BCS impact ratings that share CPU and memory resources by aligning the CIP Requirements for all systems within an ESZ or ESP and affinity to prevent sharing of CPU and memory between Virtual Cyber Assets of differing impact ratings. Do you agree with these changes? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 11, 12, and 14).

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

We agree with EEI's comments.

We do not believe that cyber infrastructure can be shared among VCAs of differing impact, trust, or security levels without rendering all VCAs on SCI susceptible to disruption by a successful attack on the VCA with the lowest level of impact, trust, or security. Although this proposal protects the CPU and memory, it still leaves the Hypervisor vulnerable. SCI needs to be limited to a single impact, trust, or security level; each level needs its own SCI. If virtualization and all its benefits are to be pursued, it cannot be at the expense of compromised security in pursuit of reducing the monetary expense of SCI by hosting mixed trust zones on a single common infrastructure.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer	No
Document Name	

Comment

This equates to not being able to use a shared virtual environment for even EACS, there would need to be dedicated environments.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

We agree with the principle and disagree with the changes. Based on our comments in the question 1, given that SCI would fall within the definition of BCS, EACMS or PACS, the hypervisor or management plane would be protected at the same level as one of the BCA, EACMS or PACS it hosts or manages. We suggest change R1 Part 1.6 to the following:

“All applicable systems shall not share CPU and memory with non-applicable systems.”

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

See Southern’s comments to previous questions.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

Where did the SDT prevent the sharing of CPU and memory between VCAs of differing impact ratings? The CPU and memory sharing come up in R1.6 and R2.6. R1.6 is only for management systems and not the actual VCAs. There is no language that the sharing cannot be across impact ratings. Also if VCAs are of differing impact ratings then the lower impact rating VCA is by proposed definition a PCA. Is the SDT proposing to not allow BCAs and PCAs to share CPU and memory on SCI?

Both R1.6 and R2.6 are not what was promised by objective and not prescriptive. As discussed at the end of response to comment #4, good policies on CPU, memory, and storage usage could address the risk associated with sharing those resources. However the SDT has prescribed that the “Thou shall not share CPU or memory” as the only means to address the risk. Both R1.6 and R2.6 have other problems which are addressed in other comments, but they are clearly prescriptive and not objective. Consider language of “Have a means to reduce risk of a VCA utilizing CPU, memory, or storage in a way that prevents other VCAs from having access to those resources.” An entity can either physically separate the systems or use policies to achieve the objective.

Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Items separated in the different ESZs should not be categorized as PCAs in order to make the new requirements feasible for implementation. Implementation of Virtual Environments requires the replacement of a certain number of cyber assets to be economically viable. Entities whose physical ESP devices do not themselves reach this threshold will have additional compliance burden and cost from changes to this standard since they will not choose the greater cost to use CIP Virtual Environments due to separate ESZ devices now coming into PCA scope.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments	

Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We agree with EEI comments. We do not believe that cyber infrastructure can be shared among VCAs of differing impact, trust, or security levels without rendering all VCAs on SCI susceptible to disruption by a successful attack on the VCA with the lowest level of impact, trust, or security. Although this proposal protects the CPU and memory, it still leaves the Hypervisor vulnerable. SCI needs to be limited to a single impact, trust, or security level; each level needs its own SCI. If	

virtualization and all its benefits are to be pursued, it cannot be at the expense of compromised security in pursuit of reducing the monetary expense of SCI by hosting mixed trust zones on a single common infrastructure	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	No
Document Name	
Comment	
We agree with EEI comments. We do not believe that cyber infrastructure can be shared among VCAs of differing impact, trust, or security levels without rendering all VCAs on SCI susceptible to disruption by a successful attack on the VCA with the lowest level of impact, trust, or security. Although this proposal protects the CPU and memory, it still leaves the Hypervisor vulnerable. SCI needs to be limited to a single impact, trust, or security level; each level needs its own SCI. If virtualization and all its benefits are to be pursued, it cannot be at the expense of compromised security in pursuit of reducing the monetary expense of SCI by hosting mixed trust zones on a single common infrastructure.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	
Please see AEP's response to Questions #1 and #4	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	

Comment

CHPD disagrees with the proposed changes. The proposed changes would require implementation of additional infrastructure in order to keep non-BES Cyber Systems out of scope. See the comments in questions #1, #2, and #4, above, for recommendations. Correction to these other areas are first needed before CHPD can evaluate the effects of the language on differing impact ratings.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource

Answer	No
Document Name	

Comment

Since “affinity” is not a defined term, and not used in the Requirement, it is difficult to respond positively to this question. We suggest that the Technical Rationale is expanding and guiding not justifying the Requirement. We request clarification.

GENERAL COMMENT – we recommend that these questions (1 – 8) should focus on what the auditor will use (Definitions and Standards), and less so on the Technical Rationale.

We agree with the concept that all tenants on the same VM host should be high watermarked against BES Cyber System impact rating.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We agree with EEI comments.

We do not believe that cyber infrastructure can be shared among VCAs of differing impact, trust, or security levels without rendering all VCAs on SCI susceptible to disruption by a successful attack on the VCA with the lowest level of impact, trust, or security. Although this proposal protects the CPU and memory, it still leaves the Hypervisor vulnerable. SCI needs to be limited to a single impact, trust, or security level; each level needs its own SCI. If virtualization and all its benefits are to be pursued, it cannot be at the expense of compromised security in pursuit of reducing the monetary expense of SCI by hosting mixed trust zones on a single common infrastructure.

Likes 0	

Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	
Comment	
See Eversource responses to Questions 1 and 4.	
Likes 0	
Dislikes 0	
Response	
Michael Puscas - ISO New England, Inc. - 2	
Answer	No
Document Name	
Comment	
ISO-NE does not agree because the concepts of shared infrastructure and affinity are not included in the requirements of the standard (e.g., “affinity” is not described or defined in the requirements). Rather, the concepts are only mentioned in the Technical Rationale. These concepts, however, should be addressed in the requirements.	
Likes 0	
Dislikes 0	

Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 5.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
See EEI’s responses to Questions 1 and 4.	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
Our concern is that this prevents responsible entities from being able to efficiently leverage emerging technologies. We propose that the protections and requirements for the highest impact VCA hosted in the shared environment should be extended to all VCAs hosted, and to the SCI.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
No, not entirely. We agree with the scenario presented, but also think other scenarios should be permitted. See Tri-State's comments on question #2 for more information.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes

Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The difference between ESP and ESZ are difficult to determine. Please provide a basis for determining the difference between the two terms.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
The definition of Shared Cyber Infrastructure does not clearly convey mixed trust is not allowed.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

None	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
The Yes response assumes that provisions will be provided to allow existing Entity implementations within NERC environments. Will Entities be provided a phased in consideration for existing architecture and the implantation guidelines be reflective of the phased in approach? Additonally, ensure all new terms are defined.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light agrees with the concept to high watermark a mixed trust environment.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	

CAISO has no additional comments regarding this question.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the prevention of CPU and memory sharing between Virtual Cyber Assets of differing impact ratings.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the modification and understands the reasoning for the implementation of no mixed-trust to handle the unique vulnerabilities of shared CPU and memory that continue to appear. While the elimination of mixed-trust will reduce some of the benefits of virtualization, vulnerabilities with shared CPU and memory demonstrated over the last couple of years indicate mixed-trust could be a significant risk to the reliable operation of the Bulk Electric System (BES), necessitating the restriction.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	Yes
Document Name	

Comment	
N&ST suggests that a contextual definition of “affinity” be included in the Technical Rational document at the very least, if not in CIP-005 itself.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees it is a best practice that VCAs of different impact ratings should not share CPU and memory.	
Likes 0	
Dislikes 0	
Response	

6. The SDT is proposing the addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3 for “Super-ESP” scenarios where single ESP’s or ESZ’s span multiple geographic locations. Do you agree with the proposed modifications? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 18, and 25-26).

Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
We disagree with the “Super-ESP” scenarios. Given that protocol tunneling can explicitly bypass security restrictions and poses a serious challenge to network security, SDT shouldn’t modify the current CIP-005 requirements to allow use tunneling protocols between sites within a super ESP without protecting devices such as switches and routers within the same ESP. For the current CIP requirements, if a super ESP is designated across multiple geographic locations, all Cyber Assets within the ESP must be identified as BCAs or PCAs, which is reasonable from a sound security practice perspective. The proposed R1.3 may not be achievable since the devices could be owned by third parties.	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	No
Document Name	
Comment	
While N&ST supports the concept of multi-site ESPs or ESZs (and we note that so-called “extended” ESPs exist TODAY), we are concerned about the fact the proposed new requirement includes no definition of “geographic location.” This omission will, in our view, likely lead to arguments about where and when the requirement would apply. Within a single building where applicable systems in a single ESP or ESZ are in different rooms? On different floors? In different buildings that are located at the same street address? In addition, N&ST believes the requirement to provide the type of protection sought by the proposed new requirement has already been established in CIP-006-6, specifically by R1 Part 1.10.	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	

We believe that the wording may create some confusion for entities in implementation. Our concern is that a new term for intelligent electronic devices is used. We recommend that a proper definition with information around what it includes be provided by the SDT.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI supports the Super-ESP concept believing it has potential benefits. We also understand that some EEI members have seen their respective Regional Entities support the concept of a Super-ESP. However, the proposed ESZ definition would need to be clarified before moving forward with the proposed exemptions for Super-ESP scenarios. (See our response to Question 1)

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 6.

Likes 0	
Dislikes 0	

Response

Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5

Answer	No
Document Name	

Comment

SDG&E supports EEI’s comments submitted on our behalf. Additionally, SDG&E requests further clarification of the term "geographical locations."

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

The requirement is potentially duplicative of CIP-006 R1.10. In addition, CIP-012 does not have a column in the requirements for Applicable Systems, but only states that Real-Time Assessment and real-time monitoring data must be protected in terms of confidentiality and integrity. CIP-005-7 is proposing to include a requirement that is applied to only Applicable Systems as listed (without clear association between systems and the data those systems manage). Because one requirement addresses concerns identified per system and the other standard addresses concerns identified per type of data, there is potential of overlapping systems / data that both standards and requirements could address. This is confusing and should be avoided where possible, particularly where both requirements identify similar security concerns, but with slightly different language.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1,3

Answer	No
Document Name	

Comment

Eversource agrees the Super-ESP concept has potential benefits; however, we do not support the concept when considered within the framework of the proposed ESZ definition, as discussed in a previous response.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource	
Answer	No
Document Name	
Comment	
We suggest reviewing the new CIP-005 Part 1.3 to determine if there is duplication or redundancy with the existing CIP-006 Part 1.10	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes that 4.2.3.3 is not needed since a simple modification to 4.2.3.2 can cover all situations. Presently the modified 4.2.3.2. is, “Cyber Assets, including third-party owned Cyber Assets, associated with communication networks and data communication links between discrete Electronic Security Perimeters or Electronic Security Zones.” CenterPoint Energy proposes that 4.2.3.2. should be modified to: “Cyber Assets, including third-party owned Cyber Assets, associated with external communication networks and external data communication links.” All Cyber Assets used for external communication networks and external data communication links should be excluded, not just those used in certain situations. With this modification, 4.2.3.3 is not needed.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No

Document Name	
Comment	
AEP is of the opinion that the Super-ESP concept has potential benefits, but we feel the ESZ definition being proposed should be clarified before moving forward with the exemptions for Super-ESP situations. Please see AEP's response to Question #1.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Dominion Energy supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
The exemption increases vulnerability in the CIP communication architecture.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	

Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the concept of Super-ESPs and the potential benefits that could be realized in implementing this concept. However, the proposed ESZ definition should be clarified or modified before moving forward with the proposed exemptions for Super-ESP scenarios.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
GSOC/OPC agrees with the addition of CIP-005 requirement R1 part 1.3, but has concerns that the wording of Exemption 4.2.3.3 is ambiguous and could result in confusion or misinterpretation relative to the excluded assets. For example, use of the phrase “associated with” when coupled with expansive terms such as “communication networks and data communication links” could result in differing interpretations and applications by different entities, e.g., one entity could view an asset or type of equipment as “associated with” “communication networks” and/or “data communication links” while others would not. This potential for confusion and multiple interpretations could be exacerbated where different regions and auditors manifest differences in application of the exemption during compliance monitoring activities. GSOC/OPC recommends that the SDT consider utilizing verbiage in	

the exception that hews more closely to the language utilized in the Technical Rationale document, i.e., transport networks. For example, the exemption could be revised as follows:

4.2.3.3. Cyber Assets, including third-party owned Cyber Assets, associated with transport networks and associated data communication links used to extend a discrete ESP or ESZ to one or more geographic location(s).

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

We agree with the specific addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3, provided the ESZ concerns posed in **Question 3** are addressed.

We agree with EEI's comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	

Comment

GTC agrees with the addition of CIP-005 requirement R1 part 1.3, but has concerns that the wording of Exemption 4.2.3.3 is ambiguous and could result in confusion or misinterpretation relative to the excluded assets. For example, use of the term “associated with” could result in differing applications by different entities, e.g., one entity could view an asset as “associated with” while others would not. This potential for confusion and multiple interpretations could be exacerbated where different regions and auditors manifest differences in application of the exemption during compliance monitoring activities. GTC recommends that the SDT consider utilizing verbiage in the exception that hews more closely to the language utilized in the Technical Rationale document, i.e., transport networks. For example, the exemption could be revised as follows:

4.2.3.3. Cyber Assets, including third-party owned Cyber Assets, associated with transport networks and associated data communication links used to extend a discrete ESP or ESZ to one or more geographic location(s).

Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	

PG&E agrees with the exception modification to include Electronic Security Zone (ESZ) in 4.2.3.2 and the addition of 4.2.3.3 to address the interconnection of discrete Electronic Security Perimeters (ESP) and ESZ for third-party Cyber Assets PG&E would not have direct control of. This will codify the creation of “Super-ESP/ESZ,” which many Entities are currently using and reduce potential compliance issues as a result of differences in opinion between Entities and Audit Teams on the creation of a “Super-ESP” under the current requirements.

PG&E also indicates the creation of Requirement Part 1.3 clearly indicates the confidentially and integrity of communications must be maintained by the Entity, even when third-party-owned Cyber Assets are being used.

Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	

Tri-State agrees with the proposed modifications.

Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Duke Energy agrees with the concept of Super-ESP as long as it is optional and backward compatible to the current CIP-005 requirement.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO has no additional comments regarding this question.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light agrees that "Super-ESP" scenarios must be addressed and accepts the proposed approach as perhaps the most appropriate one possible within the CIP Standards. At the same time, City Light is concerned that about expanding the existing confusion about "communications infrastructure" into a much less well-defined space. We have spent hours at each CIP audit explaining our approach to communications infrastructure; each time it seems we need to re-educate and convince a new team of CIP auditors. We urge that extensive examples and training—for entities and auditors alike—be developed to minimize the audit risks associated with this change, before this concept takes force in a Standard. We recommend a pilot study, similar to the regional pilots of CIP v5, with lessons learned for both industry and auditors.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	

Comment

We agree with the specific addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3, provided the ESZ concerns posed in **Question 3** are addressed.

We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO

Answer	Yes
Document Name	

Comment

We agree with the specific addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3, provided the ESZ concerns posed in **Question 3** are addressed.

We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels.

Likes 0	
Dislikes 0	

Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
We agree with the specific addition of exemption 4.2.3.3 and CIP-005 requirement R1 part 1.3, provided the ESZ concerns posed in **Question 3** are addressed. We agree with EEI comments that undefined “systems and components” is unclear. If the objective is to create a parallel term to mirror the concept of an ESP to define a virtualized environment, the definition can be simplified to “A logically isolated section of a network containing one or more VCAs.” From a security perspective we do not believe it is wise to allow mixed trust ESZs to be hosted on common hardware. We believe all ESZs on a given SCI should share the same impact, trust, or security levels.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE seeks clarification on why exemptions 4.2.3.2 and 4.2.3.3 exempt “third-party owned Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters or Electronic Security Zone…”

- For example, if a registered entity owns a generation Facility but a third party owns Cyber Assets in that Facility and those Cyber Assets have a 15-minute impact and meet the definition of a BCA. The registered entity is responsible for those BCAs.

Texas RE agrees protecting confidentiality and integrity of the data traversing communication networks and data communication links used to extend an applicable ESP or ESZ is very important and should be implemented. Logical isolation and segmenting should be implemented properly so large IP subnets are not used.

Texas RE suggests the terms “Super-ESP” and “geographic location” may not be the best terms. The reasoning for CIP-005-7 includes BES Cyber System Logical Isolation. However, the SDT is allowing “Super-ESP” concepts that could include large IP ranges. Segmenting the network properly includes smaller IP ranges and logical isolation which improves access control, monitoring, performance, and containment. In addition, Texas RE recommends defining geographic location and possibly including a threshold.

Likes 0	
Dislikes 0	

Response

Neil Swearingen - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

Not Applicable to the High Impact Control Centers.

Likes 0	
Dislikes 0	

Response

7. The SDT is proposing to retire EACMS and develop two new terms: EACS and EAMS. These terms will allow changes within the applicable systems column of the relevant requirements to allow third party monitoring. Monitoring and logging data will be handled within CIP-011 in a future posting. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. NOTE: Project 2016-02 will coordinate with Project 2019-02 (BCSI) and Project 2019-03 (Supply Chain) on this topic. (CIP-005 Technical Rationale pages 9, 10, 13, and 19).

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

Given that the CIP compliance program works fairly smoothly by implementing the existing requirements with all applicable system, it may not be necessary for splitting the EACMS and PACS into two separate devices from an ongoing compliance workload perspective. In addition, monitoring device cannot be treated the same level since some of them more critical than others. We suggest initiating a survey before making a decision for splitting.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource

Answer	No
Document Name	

Comment

We recommend keeping the EACMS term while adding the new EACS and EAMS term

EACS (External Access Control System) & EAMS (External Access Monitoring System) – we request keeping the old term / definition / applicability EACMS in addition to these two new terms / definitions / applicability. We suggest that the Entity has the flexibility to use any of these three terms / definitions / applicability to avoid forcing Entities in to costly, large changes to their documentation and training, etc.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

While it is appreciated the cost savings that could occur as a result of third party monitoring, there is no assurance that the data or even the EAMS will be protected properly.

Likes 0	
Dislikes 0	

Response
Quintin Lee - Eversource Energy - 1,3

Answer	No
Document Name	

Comment
Eversource recommends modifying the EACMS term while adding the new EACS and EAMS terms. We recommend modifying the existing EACMS to: 'Cyber Assets that perform electronic access control **and** electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems.' The Entity would be able to use these three terms as needed since some devices are used for both control and monitoring whereas some devices are only used for control or monitoring. This would avoid forcing Entities to changes to their documentation and training, etc just for a glossary term change which improves the backwards compatibility effort.

Likes 0	
Dislikes 0	

Response
Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment
While ISO-NE agrees that the current definitions associated with BES Cyber Systems do not adequately account for virtualization, ISO-NE cautions that adding new terms and definitions continues to foster an object of requirement approach instead of moving towards an information security objective based approach. It is difficult to ascertain whether the definitions are adequate and determine the impact of the new definition without seeing the revisions in the other standards/requirements, specifically CIP-007 and CIP-010. To achieve the backwards compatibility, all existing terms must remain in place. In addition, introducing the concept that assets can be have multiple classifications can have profound influence on processes and tools already implemented.

Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E requests not retiring EACMS. There may still be instances where a single asset will be categorized as both controlling and monitoring. Keeping EACMS would allow flexibility in defining the asset as one term. Alternatively, allow for dual classification as an EACS and EAMS.	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5	
Answer	No
Document Name	
Comment	
Yes, we generally agree with the concept. However, we will need to see what the changes to CIP-011 look like. In particular, R2 will need to be clear on the expectations for "disposal" of a VM. Is just deleting a VM sufficient? How does an entity prove actions were taken to prevent the unauthorized retrieval of BCSI, if we're not decommissioning the physical asset/hard disks? Will this be covered in the CIP-011 posting?	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	No
Document Name	
Comment	
N&ST disagrees with the proposal to break out monitoring functions from the existing EACMS and PACS definitions in order to serve the goal of easily accommodating third-party, possibly cloud-based, electronic and/or physical access monitoring. We strongly disagree with the rationale that "access	

monitoring” is somehow less critical, and poses less inherent risk, than “access control,” particularly in light of the fact the 2016 SANS / E-ISAC analysis of the attack on Ukrainian power grid cited a lack of monitoring as a key factor in the attack’s success.

Likes 0

Dislikes 0

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

We would like to see clarification that Cyber Assets designated as EACS are exclusively EACS and not also subject to requirements applicable to EAMS if the EACS also performs monitoring, given the understanding that EACS are more critical and will require greater security than EAMS.

Likes 0

Dislikes 0

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	Yes
Document Name	

Comment

Given the source definition, the inclusion of the term “monitor” in the Physical Access Monitoring System (PAMS) definition could be interpreted as an expansion of the scope of the existing definition and, as a result, applicable requirements. Specifically, the term “monitor” is not found/is not explicit within the current definition of Physical Access Control System (PACS). To remain consistent with the objective of merely separating the existing definition(s) without impacting scope, GSOC/OPC recommends adhering more closely to the existing verbiage when separating the current term and definition into PACS and PAMS. To achieve this, GSOC/OPC recommends referring to the language in the Technical Rationale document when finalizing this language.

Additionally, GSOC/OPC would suggest greater consistency between the definitions for PAMS/PACS and Electronic Access Control System (EACS)/Electronic Access Monitoring System (EAMS). Currently, the definitions differ significantly despite the systems performing substantially the same functions/tasks. To rectify this and ensure consistency, GSOC/OPC recommends the following revisions to EACS and EAMS:

EACS: Cyber Assets or Virtual Cyber Assets that control electronic access to a BES Cyber Asset, Electronic Access Control System, Electronic Access Monitoring System, Physical Access Control System, or Physical Access Monitoring System.

EAMS: Cyber Assets or Virtual Cyber Assets that monitor electronic access to a BES Cyber Asset, Electronic Access Control System, Electronic Access Monitoring System, Physical Access Control System, or Physical Access Monitoring System.

Likes 0

Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Please clarify with regard to the use of system tools such as AV patch management.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC

Answer	Yes
Document Name	

Comment

See EEI Comments.

Likes 0

Dislikes 0

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

We would like to see clarification that Cyber Assets designated as EACS are exclusively EACS and not also subject to requirements applicable to EAMS if the EACS also performs monitoring, given the understanding that EACS are more critical and will require greater security than EAMS.

Likes 0

Dislikes 0

Response

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO

Answer	Yes
Document Name	

Comment

We would like to see clarification that Cyber Assets designated as EACS are exclusively EACS and not also subject to requirements applicable to EAMS if the EACS also performs monitoring, given the understanding that EACS are more critical and will require greater security than EAMS.

Likes 0

Dislikes 0

Response

Kent Feliks - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP supports the changes proposed by the SDT.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
We would like to see clarification that Cyber Assets designated as EACS are exclusively EACS and not also subject to requirements applicable to EAMS if the EACS also performs monitoring, given the understanding that EACS are more critical and will require greater security than EAMS.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes

Document Name	

Comment

The proposed retirement and development of the two new terms provides additional capability at the Entity level. However, the remaining CIP Standards needs to be revised to reflect the new terms within the Applicable Systems.

There should be considerations for all CIP standards impacted by virtualization be updated concurrently to ensure efforts to make the necessary modifications to existing architecture by the entity.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment

The Exelon companies agree with the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

City Light understands and supports the change, in support of new monitoring technologies and services, but is not convinced that the EAMS term is necessary. Please consider if sufficient protection could be provided simply by defining the contents of proposed EAMS as BCSI and addressing risk that way, and/or if an EAMS is really just another type of PCA or VCA? See also response to Question 1, above.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

We agree with the retirement of the term EACMS and the creation of the two new terms, EACS and EAMS. In the interim, until all associated EACMS requirements can be updated, we believe it would be beneficial for the SDT (or another SDT) to move forward with approving the new EACS and EAMS definition but wait to retire the “EACMS” definition. We believe that all three terms could be active, and the requirements could be applied based on the applicable systems. As the requirements are updated, the SDT(s) could move away from utilizing EACMS and have EACS and/or EAMS as applicable systems instead. The ongoing delay in making the definition changes continue to have an impact on other CIP SDTs, particularly the 2018-02 CIP-008 Incident Reporting, 2019-03 CIP-013 Supply Chain, and 2019-02 BES Cyber System Information Access Management teams. Each of those teams would have benefited (or will benefit) from the updated definitions. Furthermore, the 2016-02 team would not need to continue to re-visit new or modified standards-- thus lessening the team’s burden of changes.

Likes 0	
Dislikes 0	

Response

James Brown - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

CAISO has no additional comments regarding this question.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy agrees with the retirement of EACMS and the development of new terms EACS and EAMS as long as it is optional and backward compatible to the current CIP-005 requirement.

Likes 0	
Dislikes 0	

Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	Yes
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 7.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
While we agree with the new terminology, this will require most entities to make modifications to their entire CIP program, processes, databases, GRC tools and evidence artifacts.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI support's the SDT's proposal.	
Likes 0	
Dislikes 0	
Response	

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC

Answer	Yes
Document Name	

Comment

PG&E agrees the retirement of Electronic Access Control or Monitoring Systems (EACMS) and replacement with Electronic Access Control System (EACS) and Electronic Access Monitoring Systems (EAMS) will achieve the stated goal of applying the appropriate security controls based on risk to the Bulk Electric System (BES) and allow for the use of monitoring and alerting capabilities from third-party service providers.

Request - PG&E is requesting input from the SDT on the ability of the separated EACS and EAMS to receive updates (i.e. signatures, patterns) either from PG&E-established sources or PG&E-identified trusted supplier sources using either “push” or “pull” methods. PG&E’s current understanding is receiving EAMCS updates directly from a trusted supplier source is not allowed, and would like to know if the proposed EACS/EAMS separation will allow for this update method as other Standard modifications (i.e. CIP-007) are being considered.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	

Comment

The inclusion of the term “monitor” in the PAMS definition could be interpreted as an expansion of the existing definition and associated requirements as such term is not explicit within the definition for source term associated with physical access control and monitoring (PACS). GTC recommends adhering more closely to the existing verbiage when separating the current term and definition into PACS and PAMS, and in referring to the language in the Technical Rationale document when finalizing this language.

GTC would suggest greater consistency between the definitions for PAMS/PACS and EACS/EAMS. Currently, the definitions differ significantly despite the systems performing substantially the same functions/tasks. To rectify this and ensure consistency, GTC recommends the following revisions to EACS and EAMS:

EACS: Cyber Assets or Virtual Cyber Assets that control electronic access to a BES Cyber Asset, Electronic Access Control System, Electronic Access Monitoring System, Physical Access Control System, or Physical Access Monitoring System.

EAMS: Cyber Assets or Virtual Cyber Assets that monitor electronic access to a BES Cyber Asset, Electronic Access Control System, Electronic Access Monitoring System, Physical Access Control System, or Physical Access Monitoring System.

Likes 0	

Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE is not opposed to modifying the CIP requirements to facilitate registered entities using third party monitoring services. Texas RE recognizes that third parties may be able to provide services that some registered entities do not have the skillset or staffing to perform themselves, such as 24-hour security monitoring or alerting.

Texas RE is concerned, however, that bifurcating the current term, EACMS, into the two new terms, EACS and EAMS, will allow for carve outs of one or the other which will reduce the security obligations of monitoring systems owned, operated, and maintained by registered entities. For example, a monitoring system (proposed EAMS), such as a SIEM, typically contains a large amount of the information an attacker will need to plan their attack so it should be protected by the CIP standards. The proposed bifurcation would allow an entity to carve out SIEMs. A monitoring system, such as a SIEM, would also contain the logs a registered entity would need to perform a forensics analysis of the attack. As such, it would also be a likely target in an attack on the electric grid.

If the SDT feels that registered entities are unable to make use of third party monitoring services that would improve the security and reliability of the Bulk Electric System due to the current definition of EACMS then Texas RE recommends that the SDT consider submitting a SAR to draft a new standard that covers the acceptable use of third party services.

This new standard could be modeled after CIP-013. Whereas CIP-013's purpose is to mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems this new standard's purpose could be to mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for third party management of security services provided to registered entities. This standard would codify the requirements around how registered entities can securely make use of third party monitoring services.

As part of this project, Texas RE would then recommend modifying the definition of EACMS to specify that EACMS are owned by registered entities. This modification to the definition would then unambiguously exclude third party entities from being required to comply with the other CIP standards.

Likes 0	
Dislikes 0	

Response

8. The V5TAG document request the SDT to “Clarify the IRA definition to address the placement of the phrase “using a routable protocol” in the definition and clarity with respect to Dial-up Connectivity.” Therefore, the SDT proposes modifications to the IRA definition and CIP-005 Requirement R2. These modifications will clarify scenarios where Interactive Remote Access applies to serial only devices. Do you agree? If you do not agree, please provide your recommendation and, if appropriate, technical or procedural justification. (CIP-005 Technical Rationale pages 7, 19-21, 27, and 33-37).

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant supports MRO NSRF's comments.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

See comment #10 regarding R2.1

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Remote access client has no location specified. A user could use a remote access client locally. This does not address system-to-system similar to CIP-013, and is inconsistent with CIP-013 in regards to system-to-system vs IRA.

Likes 0	

Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

With respect to Interactive Remote Access, ERCOT requests clarification as to whether the definition should be limited to only solutions using a remote access client. This appears to be very narrow and may exclude future technologies. The IRA definition and Requirement R2 do not appear to have been updated to specifically address dial-up. The removal of specifics can be misleading, especially where an entity might not consider dial-up capability to align with “remote access client.”

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

We disagree with the IRA modifications since the current IRA definition has already covered the serial only devices and devices outside of ESP, but just CIP-005 R2 has not addressed that yet except CIP-004 R5.1. In the current IRA definition: “User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol…”, the IRA definition only states the user-initiated access using a routable protocol and doesn’t say all communication sessions need to be routable. Also it doesn’t say the Cyber Asset that is accessible by a remote client has to be within ESP. For instance, when a device serially connected to a terminal server and it can be accessible by a remote client, it meets IRA definition, but current CIP-005-5 R2 doesn’t apply since R2 only apply to the cyber asset within ESP. However, for CIP-004 R5.1, it requires to revoke IRA access to High and medium impact BCS and associated EACMS and PACS, it implies EACMS or PACS may have IRA access even though they are not within an ESP. Given that current IRA definition has covered the serial only devices and devices outside of ESP, we only need to modify the applicable systems in CIP-005 R2 to address these devices. We suggest changing the applicable systems in CIP-005 R2 without changing the requirements as follows:

“High Impact BES Cyber Systems and their associated EACM, PACS and PCA

Medium Impact BES Cyber Systems and their associated EACM, PACS and PCA”

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
The proposed language does not provide clarity to serial only devices as they (serial or dial-up) is not called out in R2.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We agree with EEI's comments on the IRA definition in Question 1. The clarity requested by the SAR can be provided by changing the phrase to "using a routable or dial-up protocol." We ask the SDT to respect the scope of the SAR, and propose that if the SDT desires to clarify scenarios where IRA includes serially connected devices and security controls for these devices, this would be more appropriately handled by a future SAR requesting authorization to do so.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	No
Document Name	
Comment	
N&ST believes the proposed modification of "IRA" has been watered down to the point where it basically defines "Interactive Remote Access" as remote access that's interactive. While we concur with removing as much "requirements-like" language from Glossary definitions, we believe the revised definition should retain the information that "IRA" is access to a BES Cyber System or associated applicable system and that it is initiated from outside the ESP or ESZ where the system being accessed is located.	
Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	CIP 005_Q8 Diagram.pdf

Comment

Tri-State does not agree. The removal of the ERC characteristic from the definition of IRA will bring into scope several types of serial communications links that should not be defined as having IRA.

Several examples include:

- The RTU owned by entity "A" has ERC and IRA. There is also a serial communications link between the RTU owned by entity "A" and an RTU owned by entity "B" inside the substation control house. Under the new IRA definition the RTU owned by entity "B" has an IRA link from entity "A".
- The RTU in a substation control house has a serial communications link to the control center. At the control center the serial communications link is connected to the SCADA network. Under the new IRA definition this RTU has IRA.
- The RTU owned by entity "A" inside a substation control house with a serial communications to a control center owned by entity "B". At the control center owned by entity "B", the serial communications link is converted to routable protocol and connected to the SCADA network. Under the new IRA definition this RTU owned by entity "A" has IRA to the SCADA network owned by entity "B".
- An RTU in a substation control house with IRA has a serial link to a cyber asset in the substation yard. Under the new IRA definition the cyber asset in the control house yard has IRA.

We believe the risk is at the initial point where Ethernet and serial merge. Current requirements require authentication which mitigate the risk. This change to IRA does not provide additional protection but does significantly increase scope. By increasing scope we divert limited resources that would be better used at higher risk areas.

In addition, IRA for serial communications may bring into scope the IP-to-Serial connections from an EMS (front-end processor) application server down to the RTU at a substation. One could argue that an EMS user has IRA to the RTU from the EMS front-end processor server. This communication should be excluded from the IRA definition and this situation needs to be addressed by the SDT. See the uploaded diagram for further details:

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

As written, the definition of IRA can apply to an RDP connection from one asset inside of an ESP to another asset inside of the same ESP since a User is initiating access and employing a remote access client. This would render R2.1 impossible to follow for a majority of RDP connections in a given system. We propose that the language about the connection not originating from a IS, within an ESP or at an access point should remain to clarify that point.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	No
Document Name	
Comment	
Interactive Remote Access: Request clarification of whether the definition should be limited to only solutions using a remote access client. This appears to be very narrow and may exclude future technologies. The IRA definition and Requirement R2 does not appear to have been updated to specifically address dial-up. The removal of specifics can be misleading, especially where an entity may not consider dial-up capability to align with “remote access client."	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
See EEI’s response to Question 1 above.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	

Comment

Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 8.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not generally agree with the modifications to the IRA defintion and CIP-005 Requirement R2. The definition removes "using routable protocol" and incorporates IP to serial conversion scenarios or serial only scenarios. Since serial connections can now be treated as IRA, this may cause a burden on the business units who support serial connected devices.

Likes 0	
Dislikes 0	

Response

Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5

Answer	No
Document Name	

Comment

SDG&E supports EEI’s comments submitted on our behalf.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

The new definition is ambiguous and opens up a broad discussion of what a remote access client is. The new definition does not provide clarity. In addition, the definition is not backwards compatible.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
Regarding the Interactive Remote Access definition: Request clarification of whether the definition should be limited to only solutions using a remote access client. This appears to be very narrow and may exclude future technologies. The IRA definition and Requirement R2 does not appear to have been updated to specifically address dial-up. The removal of specifics can be misleading, especially where the entity might not consider dial-up capability to align with “remote access client.”	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	

AZPS believes this scenario may lead to the determination that serial assets utilizing a session termination gateway may be incorrectly subject to requirements intended for ERC assets. This will lead to unnecessary effort in conforming to standards that have no additional security benefit, e.g. CIP007-6 R1.1.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with EEI's comments on the IRA definition in Question 1. The clarity requested by the SAR can be provided by changing the phrase to "using a routable or dial-up protocol." We ask the SDT to respect the scope of the SAR, and propose that if the SDT desires to clarify scenarios where IRA includes serially connected devices and security controls for these devices, this would be more appropriately handled by a future SAR requesting authorization to do so.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	No
Document Name	
Comment	
Please see AEP's response to Question #1	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	No

Document Name	
Comment	
We agree with EEI’s comments on the IRA definition in Question 1. The clarity requested by the SAR can be provided by simply changing the phrase to “using a routable or dial-up protocol.” We ask the SDT to respect the scope of the SAR, and propose that if the SDT desires to clarify scenarios where IRA includes serially connected devices and security controls for these devices, this would be more appropriately handled by a future SAR requesting authorization to do so.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We agree with EEI’s comments on the IRA definition in Question 1. The clarity requested by the SAR can be provided by simply changing the phrase to “using a routable or dial-up protocol.” We ask the SDT to respect the scope of the SAR, and propose that if the SDT desires to clarify scenarios where IRA includes serially connected devices and security controls for these devices, this would be more appropriately handled by a future SAR requesting authorization to do so.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	

Answer	No
Document Name	
Comment	
Interactive Remote Access: Request clarification of whether the definition should be limited to only solutions using a remote access client. This appears to be very narrow and may exclude future technologies. The IRA definition and Requirement R2 does not appear to have been updated to specifically address dial-up. The removal of specifics can be misleading, especially where entity might not consider dial-up capability to align with “remote access client.”	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern requests the SDT take steps to ensure that the scope of IRA is clear and doesn’t bring in cyber assets not currently covered under this definition. For example, today the IRA definition implies remote access “into an ESP”, yet EACMS and PACS are not required to be in an ESP today. By virtualizing EACS or PACS, does this create IRA to those asset types if they are required to be in an ESZ? Is all “remote” access into an ESZ going to be considered IRA going forward for virtualized EACS and PACS, even if those assets aren’t on the same SCI as a h/m BES Cyber System? Or if they are ONLY hosted on SCI with other EACS or PACS, respectively? These types of questions appear to be questions and confusion as to the intended applicability of requirements to specific virtualized systems that the SDT should help clarify in subsequent rounds of commenting/balloting.	
Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	Yes
Document Name	

Comment

GSOC/OPC provides the following comments for the SDT’s review and consideration:

- To ensure that the definitions remain neutral to a particular implementation method, GSOC/OPC recommends that the SDT revise the definition of Interactive Remote Access to include “or other remote access technology.”
- GSOC/OPC is concerned about the expansion of definitions to address serial to IP connectivity without the inclusion of proposed implementation timelines/timeframes.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	

Comment

· To ensure that the definitions remain neutral to a particular implementation method, GTC recommends that the SDT revise the definition of Interactive Remote Access to include “or other remote access technology.”

· GTC is concerned about the expansion of definitions to address serial to IP connectivity without the inclusion of proposed implementation timelines/timeframes.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC

Answer	Yes
Document Name	

Comment

PG&E agrees the proposed modifications correctly address the risks of Interactive Remote Access (IRA) using connection methods other than “a routable protocol” which is absent from the current CIP-005-5 and -6 Standards. IRA access using Dial-up, serial, or IP-to-Serial connection methods have the same risk as those employing a routable protocol.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

City Light recognizes the request to address “routable protocol” and “Dial-up Connectivity” but does not agree that this revision is the time and place to do so. The proposed changes to “routable protocol” and “Dial-up Connectivity” may have significant impact to entities, and no justification has been provided about whatever is the security concern driving the proposed changes. These changes also are likely to be lost in all the other changes aimed at accommodating virtualization. For these reasons, City Light strongly urges that all changes regarding “routable protocol” and “Dial-up Connectivity” be struck from this revision and proposed separately. They are worthy of attention on their own, not as part of this even larger, and largely different, effort.

It could be as simple as preparing for comments (and perhaps ballot) a separate proposed version of CIP-005, that includes only the proposed changes to “routable protocol” and “Dial-up Connectivity,” without any of proposed virtualization changes.

Such a change may also promote acceptance of the changes proposed in support of virtualization, by removing any chance for ***NO*** *ballots based on concern about these unconnected changes.*

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	Yes
Document Name	

Comment

Recommend the SDT provide clarification to the IRA definition as it creates confusion and does not appear to address Dial-Up Connectivity. Will Entities be provided a phased in consideration for existing architecture and the implantation guidelines be reflective of the phased in approach?

Likes 0	
Dislikes 0	

Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 3,5,6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
Not Applicable to the High Impact Control Centers.	
Likes 0	
Dislikes 0	
Response	

9. The SDT is proposing modifications to CIP-005 Requirement R1. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rational pages 22-32).

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	
Comment	
We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.	
Likes 0	
Dislikes 0	
Response	

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	
Comment	

We disagree with modifications to CIP-005 R1 (See our comments in question 1 & 3).

· For R1.1, if SDT still wants network layer protection for EACMS and PACS, we suggest changing the CIP-005 R1.1 applicable systems to include EACMS and PACS.

· For R1.2, if STD intends to allow inbound and outbound access control either at network perimeter level or local device level, the applicable system should be changed as follows:

o Electronic Security Perimeter

o High Impact BES Cyber Systems and their associated EACM, PACS and PCA

o Medium Impact BES Cyber Systems and their associated EACM, PACS and PCA

Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment	
ERCOT offers the following items for consideration: Part 1.1 Measure: An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems. Add in “Cyber Assets connected via a routable protocol within each ESP or Cyber Assets and virtual Cyber Assets contained within the ESZ.” Part 1.2: Regarding the exclusion of time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE), this needs to be clarified to address situations where communication is coming into a BCS from a remote location. It appears that some sort of “rule” would be required for this communication. Part 1.3: Break the exclusion away from the requirement to add emphasis. See 1.2. Part 1.6 Measure: Enforcing authentication looks to be a new requirement created within a measure. The requirement and measure do not align.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Please see Southern’s response to previous questions.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	

For R1.1 we disagree with PACS and EACS hosted on SCI being in scope. A PACS or EACS that is virtualized is not at any higher risk than the physical counterpart that does not have a requirement to have communications to and from controlled. As stated in comment #4 if the concern is PACS or EACS hosted on SCI that also hosts HIBCS or MIBCS then they are covered by definition as an associated PCA. Per comment #3 we believe ESP can be retired and thus the requirement language could drop ESP.

For R1.2 we agree with the premise. Again, ESP could probably be dropped from Applicable Systems.

The structure of R1.1 and R1.2 punish entities that have defense in depth with a larger perimeter and then host-based or zone firewalls deployed. Under the proposed requirement if an ESZ within another ESP or ESZ was not properly configured with access permissions yet the larger perimeter or zone was then it is still a violation. The standard needs to be objective based of requiring logical access permissions to HIBCS, MIBCS, and associated PCAs. In the defense in depth model if at least one of the perimeter or zones are configured correctly then the objective is accomplished. Under the proposed CIP requirement if one is but another isn't then it is a violation when in fact there was no risk to the Bulk Electric System. Supporting the defense in depth model encourages entities to deploy zones within zones to reduce compliance risk and increase security. Not supporting the defense in depth model will create a driver for entities to reduce compliance risk by having only one zone. While compliance risk has been accomplished the security of the Bulk Electric System suffers because of single point of failure encouraged by the compliance risk. Proposed R1.2 is still prescriptive not objective based. A way to address the issue could be to have R1.2 have the Applicable Systems of HIBCS, MIBCS and associated PCA and SCI. The requirement would be "At least one ESP or ESZ protecting the Applicable System, require inbound or outbound logical access permissions, including the reason for granting access, and deny all other logical access by default. The access permissions can exclude time-sensitive protection or control functions…." This would allow entities to have defense in depth but only need to prove that at least one of the layers had protections in place.

We agree with the premise of R1.3. This is a gap in CIP-012.

We disagree with the applicable systems in R1.4. If physical PACS and EACS do not have Dial-Up Connectivity requirements then why do the virtualized PACS and EACS have such requirements. Again as stated before PACS or EACS sharing the same SCI as HIBCS or MIBCS are also by definition PCAs.

For R1.5 we agree with the requirement but disagree with the Applicable Systems. This should have the same Applicable Systems as proposed R1.2 for conformity purposes.

For R1.6 it is unclear what risk the SDT is trying to address. Why are management systems of SCI hosting HIBCS or MIBCS only called out. A physical BCA could have a baseboard management controller. Is there a reason its management system doesn't have similar restrictions? Management systems do not exist only on virtual infrastructure. Also as mentioned before it is unclear what the SDT means by management systems. We strongly urge the SDT to make this a defined term. For example SCADA is typically managed from within the same GUI operators use and cannot be separated. More clarification is needed for this requirement.

Likes 0	
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	No
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
All CIP standards impacted by virtualization should be updated concurrently. The efforts for the entities to adopt these changes would be significant.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
Reclamation recommends if replacing Electronic Security Perimeter with Logical Isolation, this term should be added to the NERC Glossary of Terms. Logical Isolation is not a NERC defined term and has not been added as a new definition within this standard revision proposal.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	

Answer	No
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

SWG offers the following items for consideration.

- Part 1.1 Measure: An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems. Add in “Cyber Assets connected via a routable protocol within each ESP or Cyber Assets and virtual Cyber Assets contained within the ESZ.”
- Part 1.2: Regarding the exclusion of time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE), this needs to be clarified to address situations where communication is coming into a BCS from a remote location. It appears that some sort of “rule” would be required for this communication.
- Part 1.3: Break the exclusion away from the requirement to add emphasis. Look at 1.2.
- Part 1.6 Measure: Enforcing authentication looks to be a new requirement created within a measure. The requirement and measure do not align.

Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Oncor supports EEI's comment.	
Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.

Likes 0

Dislikes 0

Response

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO

Answer	No
Document Name	

Comment

We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.

Likes 0

Dislikes 0

Response

Kent Feliks - AEP - 3,5

Answer	No
Document Name	

Comment

Please see AEP’s response to Question #1

Likes 0

Dislikes 0

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

Revise Requirement R1, Part 1.1 to, “All applicable systems shall reside within one or more, or on the logical perimeter of defined ESPs or ESZs.”

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Internet Protocol (IP) is not the only risk that should be addressed. While it is the dominant routable protocol in modern use, multiple other routable protocols exist (for example, IPX, Appletalk, etc.), as well as “layer 2” non-routable protocols that nonetheless provide a capability for conveying malicious code and infiltrating exploitable data.

Also, the R1 table title needs to be updated, from ESP to Logical Isolation.

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	

Comment

CHPD cannot agree with the changes to R1 at this time. With the current wording, it is difficult to realize implementation and successful compliance of the proposed changes without additional clarification of the new terminology and its application to other standards. Additionally, CHPD believes that the current definition for Shared Cyber Infrastructure discourages the use of virtualization for BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource

Answer	No
Document Name	

Comment

Part R1.2 – request clarification. There seems to be a gap between R1.2’s logical access permission and data diodes; because data diodes do not use/need logical access permission. How can an Entity pass an audit while using data diodes?

Part 1.2 and 1.3 – we request removing the IEC 61850 language from the Requirement since that other non-NERC Standard could change on its own. We suggest moving these exemptions into this Standards Exemptions Section (4.2.3)

Part R1.4 – the new Requirement remove the need for a mitigation plan. The Entity only needs to provide evidence the system is not capable. While we agree with intent of removing TFEs, we suggest these new words are less secure

Part 1.6 – request clarification. We believe the Requirement wants to say that the Intermediate Systems and the BES Cyber Systems must be on different virtual machine hosts.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The addition of "routable Internet Protocol (IP) communications" to eliminate storage transport protocols, does not take into account that there are known attacks on these protocols that could impact the systems utilizing these storage protocols.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
The Exelon companies agree with the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1,3	
Answer	No
Document Name	
Comment	
See Eversource response to Question 1.	
Likes 0	
Dislikes 0	
Response	
James Brown - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO offers the following items for consideration;	

- Part 1.1 Measure: An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems. Add in “Cyber Assets connected via a routable protocol within each ESP or Cyber Assets and virtual Cyber Assets contained within the ESZ.”
- Part 1.2: Regarding the exclusion of time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE), this needs to be clarified to address situations where communication is coming into a BCS from a remote location. It appears that some sort of “rule” would be required for this communication.
- Part 1.3: Break the exclusion away from the requirement to add emphasis. Look at 1.2.
- Part 1.6 Measure: Enforcing authentication looks to be a new requirement created within a measure. The requirement and measure do not align.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

R1 is potentially duplicative of CIP-006 R1.10. A review should be performed to ensure that there is no overlap and that the requirement is necessary.

For Part 1.1: The language under “Measures” currently states “[a]n example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems.” The following should be added: “Cyber Assets connected via a routable protocol within each ESP or Cyber Assets and virtual Cyber Assets connected within the ESZ.”

For Parts 1.2 and 1.3: Excluding communications using protocol IEC TR-61850-90-5 R-GOOSE is inappropriate. Perhaps use the capability of the system in this instance.

For Part 1.3: Including the CIP-012 exclusion within the requirement language overly complicates the requirement. Exclusions should be listed in the Exemptions section. CIP-012 is written without the applicability section and this requirement is asset based.

For Parts 1.1, 1.4, and 1.5: It’s confusing to have protections applied to virtualized assets but not applied to the physical assets with the same classification (i.e. PACS hosted on SCI, EACS hosted on SCI, PACS, & EACS).

For Part 1.6: The language under “Measures” includes enforcing authentication, but that is not in the requirement. Thus, “authentication” should be deleted from the measure. Also, the term “management plane” comes up in the requirement statement itself, but it is only defined in the Technical Rationale. Please consider adding either a definition of “management plane” or include specification of management and data planes as part of the SCI definition to support compliance with CIP-005-7 R1.6. At a minimum, each should be defined if they are gong be part of the requirement. This could be accomplished by adding something like the following to the SCI definition: “This includes its management systems that support configuration of policy for sharing of CPU, memory, and storage. This also includes the management plane that supports carrying instructions and status for sharing of CPU, memory, and storage.”

Likes 0	
Dislikes 0	

Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	No
Document Name	
Comment	
SDG&E supports EEI’s comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	
Answer	No
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 9.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
See EEI’s response to Question 1 above.	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	No
Document Name	

Comment

MISO offers the following items for consideration.

Part 1.1 Measure: An example of evidence may include, but is not limited to, a list of all ESPs or ESZs with all uniquely identifiable applicable systems. Add in “Cyber Assets connected via a routable protocol within each ESP or Cyber Assets and virtual Cyber Assets contained within the ESZ.”

Part 1.2: Regarding the exclusion of time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE), this needs to be clarified to address situations where communication is coming into a BCS from a remote location. It appears that some sort of “rule” would be required for this communication.

Part 1.3: Break the exclusion away from the requirement to add emphasis. Look at 1.2.

Part 1.6 Measure: Enforcing authentication looks to be a new requirement created within a measure. The requirement and measure do not align.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

According to how we interpret the new R1.1, any PAC or EAC that is virtualized will have to be placed inside of an ESP or ESZ, but the physical PACs and EACs do not have that same requirement. We believe that this creates a discrepancy in protection requirements between virtual and physical PCs. We propose that if SCI devices host BCAs or PCAs then the SDT should clarify this in the definition. Currently it applies to SCI that host VCAs inside and outside the ESP.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	

Comment

No, Tri-State does not agree with CIP-005-7 R1.6.

Regarding 1.6 we would like more clear definitions to better understand the description of management systems, management plane, and data plane. Would like examples.

As stated in the measures of CIP-005-7 R1.6, a hypervisor could be the management system, which would essentially share CPU, Memory, Disk and network resources with the hosting VMs if there is no traditional “management system.” In some cases, the hosting platform is a multi-purpose operating system such as Windows or Linux. The same argument could be applied to the containers.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC provides the following comments for the SDT’s review and consideration:

· In the Measures column for R1.1, GTC recommends capitalizing “applicable system” for consistency with previous column and other sections within the standard.

· In the Measures column for R1.2, the “each access rule” revision could be interpreted as an expansion of responsibilities. Where more than 1 rule is grouped together to form the access policy to be effected, the revised requirement could be interpreted to require a “reason” be assigned to each line in a grouping as opposed to the overall rule for the access policy resulting from the grouping. To ensure that the reliability standards present the “what,” and not the “how,” GTC recommends that the SDT review this language closely and clarify the intent. An example clarification is provided below for the SDT’s consideration:

An example of evidence may include, but is not limited to, architectural diagrams that detail how network communication is limited and a list of rules (firewall, access control lists, software defined policies, etc.) that demonstrate that only permitted access is allowed and that each access rule or policy (as applicable) has a documented reason

· Relative to R1.3, the language in the requirement too closely mirrors the language in the exception, which could result in ambiguity between what is excluded and what is included in applicability. GTC recommends that the SDT consider clarification.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	No
Document Name	

Comment

N&ST notes the proposed wording in Part 1.1 opens the possibility of defining a BCS that comprises BCAs in different ESPs or ESZs. We believe the SDT needs to better articulate the benefits of allowing this and should also address what the Technical Rationale document refers to as the risk of “side channel” attacks.

N&ST also notes that making virtualized EACS devices subject to R1 Part 1.1 would preclude using one to provide access control for a conventional, IP-based ESP.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	Yes
Document Name	

Comment

GSOC/OPC provides the following comments for the SDT’s review and consideration:

- In the Measures column for R1.1, GSOC/OPC recommends capitalizing “applicable system” for consistency with previous column and other sections within the standard.
- In the Measures column for R1.2, the “each access rule” revision could be interpreted as an expansion of responsibilities. Where more than 1 rule is grouped together to form the access policy to be effected, the revised requirement could be interpreted to require a “reason” be assigned to each line in a grouping as opposed to the overall access policy resulting from the grouping. To ensure that the reliability standards present the “what,” and not the “how,” GSOC/OPC recommends that the SDT review this language closely and clarify the intent. An example clarification is provided below for the SDT’s consideration:

An example of evidence may include, but is not limited to, architectural diagrams that detail how network communication is limited and a list of rules (firewall, access control lists, software defined policies, etc.) that demonstrate that only permitted access is allowed and that each access rule **or policy (as applicable)** has a documented reason

- Relative to R1.3, the language in the requirement too closely mirrors the language in the exception, which could result in ambiguity between what is excluded and what is included in applicability. GSOC/OPC recommends that the SDT consider clarification.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	Yes
Document Name	

Comment

1. Existing implementations that have mixed trust may require work to align trust levels once the new requirement goes live. Will Entities be provided a phased in consideration for existing architecture and the implantation guidelines be reflective of the phased in approach?
2. The requirement reads as if the isolation model can be only ESP or ESZ. Is it possible to implement a blended model, assuming all requirements are met for both implementations, or is it exclusive? It can be envisioned where both would come in to play for certain migration scenarios.   Is it possible that a Cyber Asset may appear in two or more ESZ, assuming identical trust level, or is a Cyber Asset restricted to only one ESZ?

There should be considerations for all CIP standards impacted by virtualization be updated concurrently to ensure efforts to make the necessary modifications to existing architecture by the entity.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

City Light generally supports the proposed R1 modifications, with the exceptions discussed above under Questions 2-7, and the overarching concerns discussed in Questions 1 and 13

Likes 0	
Dislikes 0	

Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
While we understand the need to identify an Electronic Access Point is no longer the only model for addressing network access control with the proposed updates, if a firewall performs the “logical isolation of an ESZ or ESP”, we are not sure how it can also reside within the defined ESP. Part 1.1 requires, if we understand the definition of Shared Cyber Infrastructure correctly (to include existing firewall that are associated with an EAP), that those firewalls (considered SCIs) must “reside within one or more defined ESPs or ESZs.” Additionally, for Part 1.6, since Shared Cyber Infrastructure includes existing firewalls, it would be helpful to define or expand on what “that hosts BES Cyber Systems” means for those already existing firewalls (non-virtual). As tedious as it might sound, adding words such as “that hosts”, without explicitly expressing what the intent of the word is, causes issues with the entities and the regions. It would be prudent to get away from terms can be construed in different ways or that can change the execution of the requirement depending on how they are interpreted.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the modifications to CIP-005 Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	

PG&E agrees with the modifications and change in approach to “logical isolation” since it would apply to the current implementation of CIP-005 (backward compatibility) and the proposed modifications to clearly allow for the use of virtual technology.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Part 1.1 - Texas RE noticed R1.1 is not a requirement to create ESPs or ESZs. Part 1.1 requires that entities place their applicable systems within a defined ESP or ESZ. The creation of the ESP or ESZ is an inferred requirement. Texas RE recommends there be a specific requirement for entities to create and/or define ESPs and/or ESZs. Texas RE recommends the language to be modified to “Define/Create and implement ESPs or ESZs for all applicable systems”. Additionally, Texas RE suggests PACS and EACS not hosted on SCI should be included in this requirement.

Part 1.2 – If the drafting team chooses not to modify Part 1.1 to explicitly require the creation of ESPs and ESZs, Texas RE recommends modifying Part 1.2 to the following. Texas RE proposes that the applicable systems in R1.2 be defined as:

Electronic Security Perimeters and Electronic Security Zones in which one or more of the following reside:

High Impact BES Cyber Systems and their associated:

PCA

SCI

PACS hosted on SCI

EACS hosted on SCI

Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated:

PCA

SCI

PACS hosted on SCI

EACS hosted on SCI

Part 1.4 – Texas RE recommends PACS and EACS not hosted on SCI also be included in this requirement since they are just as important for security as PACS and EACS hosted on SCI.

Part 1.5 states “Have one or more methods for detecting known or suspected malicious routable Internet Protocol (IP) communications to or from ESPs or ESZs.” Texas RE disagrees that detection of malicious communications is restricted to routable IP communications. Most modern IPS and IPS sensors inspect Layer 2 (non-routable) and Layer 3 (routable) traffic, and include deep packet inspection. There are layer 2 attacks such as MAC address flooding, DHCP server spoofing, Man-in-the-middle attacks, and IP host spoofing that should be monitored. Texas RE recommends the language to be modified to “Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications to or from ESPs or ESZs.

The Technical Rationale on page 28 states “The use of the phrase “routable Internet Protocol (IP) communications” is intended to eliminate internal storage transport protocols including, but not limited to Fibre Channel, iSCSI, and InfiniBand from the scope of this requirement as well as serial communications.” However, Fibre Channel and iSCSI can both operate at layer 3 of the OSI Model using routable protocol (TCP/IP).

Part 1.5 – Texas RE recommends PACS and EACS not hosted on SCI also be included in this requirement since they are just as important for security as PACS and EACS hosted on SCI.

Part 1.6 states “Management systems may only share CPU, memory, or ESZ or ESP with other management systems and the management plane.” On page 11 of the Technical Rationale there is the statement: “This inclusion is intended to ensure that devices that provide logical isolation for an ESZ or ESP, and therefore have an associated risk, have protection for the **associated management systems (management plane)** as required by Part 1.6.” Texas RE seeks clarification on the use of the words “management systems” and “management plane”. The SDT may consider defining these term(s) to improve clarity and reduce ambiguity.

Likes 0	
Dislikes 0	

Response

10. The SDT is proposing modifications to CIP-005 Requirement R2. Do you agree with these changes? Please provide comments to support your response. (CIP-005 Technical Rationale pages 33-37).

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	No
Document Name	

Comment

Alliant supports MRO NSRF's comments.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

First some entities have over declared ESPs (those without any BCS) so remote access from those ESPs do not have to traverse an Intermediate System. The language change to R2 main would affect these entities.

For R2.1 we agree with the addition of SCI to the applicable systems. However there a a couple of problems. The first is regarding IRA itself. The new IRA definition is “User-initiated access by a person employing a remote access client.” The requirement is to ensure IRA (per R2 main originating outside the ESP or ESZ) is through an Intermediate System. Does this mean TCAs are no longer allowed? A TCA can be outside the ESP or ESZ if it is a stand-alone device cabled to a BCA, or associated PCA or SCI. The TCA could employee software the allows access to the BCA or associated PCA or SCI. This could be considered Interactive Remote Access as the TCA employed a remote access client. Consider having an exclusion in R2 main of “for all remote access that originates from outside of any of the entities’ ESP’s or ESZ’s containing high or medium impact BES Cyber Systems or associated SCI *excluding directly connected TCAs*.”

The other problem is with MIBCS. The webinar mentioned the change was to include those MIBCS that were serial but elsewhere in the communication path had a serial to IP conversion. Some technicians use test sets or other devices to troubleshoot the communication to RTUs, HMIs, and data concentrators. Typically this is done on site. It is unclear with the proposed definition how this troubleshooting tool could still be used in a compliant manner. The access is user-initiated using a client tool and it isn’t within the ESP or ESZ and it isn’t through an Intermediate System. Typically, this work is done on the SCADA port using a SCADA protocol (i.e. DNP 3.0, Modbus, Series V, Conitel). These ports are typically restricted to just the SCADA protocol and do not provide remote access to actually reconfigure the device. This may be a problem with the current standard but it is more evident in the proposed standard. A suggestion would to be revise the proposed IRA definition to clarity what the remote access client can access or modify like the configuration of the device.

We agree with proposed R2.2 and R2.3.

For R2.4 and R2.5, again we disagree with PACS and EACS hosted on SCI being included in Applicable Systems. As stated, before PACS or EACS sharing the same SCI as HIBCS or MIBCS are also by definition PCAs. The purpose of CIP-005 is “To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication.” The purpose does not include a statement about protecting communication to PACS and EACS hosted on SCI. Again, if the PACS and EACS do not share SCI with a HIBCS or MIBCS then what is the concern. If there is a concern, then both physical and virtual need to be protected. Otherwise it is already address as those PACS and EACS that share SCI with HIBCS or MIBCS are also by definition PCAs.

We disagree with R2.6. This is beyond the stated purpose of CIP-005. “To protect BES Cyber Systems against compromise by allowing only known and controlled communication to and from the system and logically isolating all other communication.” The purpose is not to protect IS from compromise such as side channel attacks which the rationale indicates this requirement addresses. Why are only IS called out to prevent side channel attacks? Why are EACS and PACS hosted on SCI not also called out? The risks identified on page 37 of the rationale are not any that impact a BCS or even the BES itself, but only the Intermediate System. Thus, it should not be a Bulk Electric System Reliability Standard.   Also, it is unclear how an IS can even be within an ESZ or ESP.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

While Southern supports the recommendations made by the V5TAG to include dial-up connectivity whenever such connectivity is used for Interactive Remote Access, the use of the proposed new terms ESZ and SCI need to be clarified and modified as discussed in our response to previous questions.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT offers the following items for consideration:

R2: The leading requirement could be clearer. ERCOT suggests the SDT consider "Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management,* per system capability." The remaining language should be addressed in the applicability or requirement language in the table.

Part 2.1: Consider "User-initiated access by a person employing a remote access client." Revision of the definition may be necessary to address non-traditional remote access methods that people might not recognize. The requirement does not specify what you accessing with IRA.

Part 2.2: The lack of a definition for confidentiality and integrity could lead to inconsistency of interpretation and implementation. ERCOT suggests the SDT consider adding more clarity to the requirement language.

Part 2.4: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?

Part 2.5: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?

Part 2.6: ERCOT requests the SDT clarify why storage was not included in the requirement scope. It appears that an Intermediate System can now be in the same ESP or ESZ as the BES Cyber Systems they are protecting. Is this intentional?

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer	No
Document Name	

Comment

We disagree with modifications to CIP-005 R2 (See our comments in question 8).

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	No
Document Name	
Comment	
The current term of “encryption” provides confidentiality and integrity. Calling these out separately could cause challenges to demonstrate compliance.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
GSOC/OPC is concerned that the use of “remote access client” in the definition for Interactive Remote Access may unnecessarily limit the use of available remote access technologies. To ensure that the requirement focusses on the “what” and not the “how,” GSOC/OPC recommends the addition of “or other remote access technology to the current use of “remote access client.” Similarly, GSOC/OPC is concerned that in R2.2, the use of the term “the client” may also be unnecessarily limiting or technology-specific. Accordingly, GSOC/OPC recommends that SDT revise R2.2 and suggests the following example language: Protect the confidentiality and integrity of Interactive Remote Access between the **remote access client or technology** and the Intermediate System.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.	
Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC is concerned that the use of “remote access client” in the definition for Interactive Remote Access may unnecessarily limit the use of available remote access technologies. To ensure that the requirement focusses on the “what” and not the “how,” GTC recommends the addition of “or other remote access technology to the current use of “remote access client.” Similarly, GTC is concerned that in R2.2, the use of the term “the client” may also be unnecessarily limiting or technology-specific. Accordingly, GTC recommends that SDT revise R2.2 and suggests the following example language:

Protect the confidentiality and integrity of Interactive Remote Access between the remote access client or technology and the Intermediate System.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	

Comment

Tri-State does not agree. R2 includes wording for “all remote access” and we believe it should not be all-inclusive. R2 should be only applicable to routable communication.

Additionally, we have the same disagreement to these changes as our response to question #2. Regarding Intermediate Systems in R2.6, the standard needs to allow for situations where a traditional “management system” is not used.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	No
Document Name	

Comment

As written, R2.1 requires SCI access to go through an IS. Since SCI includes firewalls, you would be required to limit access to the firewall to an IS only. Technically, firewalls are the measure most would use to limit down the access. Due to a firewall's location on the perimeter of the ESP, it is not easy to limit what devices have access to it without adding a secondary device in front of it.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	No
Document Name	

Comment

MISO offers the following items for consideration.

R2: Clarify the leading requirement. Proposed language: “Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management,* per system capability.” The remaining language should be addressed in the applicability or requirement language in the table.

Part 2.1: Consider “User-initiated access by a person employing a remote access client.” May need to work the definition to address non-traditional remote access methods that people might not recognize. The requirement does not specify what you accessing with IRA.

Part 2.2: Lack of definition of confidentiality and integrity could lead to inconsistency of interpretation and implementation. Consider adding more clarity to the requirement language.

Part 2.4: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?

Part 2.5: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?

Part 2.6: Please clarify why storage was not included in the requirement scope. In reading this, it appears that an Intermediate System can now be in the same ESP or ESZ as the BES Cyber Systems they are protecting. Is this intentional? In addition, significant architectural work may be required by some entities to comply with this.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No

Document Name	

Comment

While EEI supports the recommendations made by the V5TAG to include dial-up connectivity whenever such connectivity is used for Interactive Remote Access, the use of the proposed new terms ESZ and SCI need to be clarified as discussed in our response to Question 1.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	No
Document Name	

Comment

Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 10.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not generally agree with the modifications to CIP-005 Requirement R2. CIP-005/Part 2.1 - Per definition of Interactive Remote Access, if the user is employing a remote access client even though the individual is initiating the request from within an ESP, it is considered IRA and needs to go through Intermediate Systems. This creates extra burden on the entities.

CIP-005/Part 2.3 - This requirement requires multi-factor authentication to Intermediate System. This may be reaching outside of the CIP scope (for example, the situation where an individual is simply accessing the intermediate system without needing to access BES Cyber Asset or Virtual Cyber Assets).

Likes 0	
Dislikes 0	

Response

Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5

Answer	No
Document Name	

Comment

SDG&E supports EEI’s comments submitted on our behalf.

Likes 0

Dislikes 0

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

For Parts 2.1, 2.4, and 2.5: All of the requirements should have the same applicable systems; in addition, the acronyms used within the requirements should be spelled out.

For Part 2.6: Part 2.6 is incompatible with consolidation efforts as it requires separate SCI for IS. This prescribes technology without providing protective value. Part 2.6 should be removed to allow consolidation of IS with other classification on an SCI.

Likes 0

Dislikes 0

Response

James Brown - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO offers the following items for consideration;

- R2: The leading requirement could use revision to be clearer. Consider, “Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management,* per system capability.” The remaining language should be addressed in the applicability or requirement language in the table.
- Part 2.1: Consider “User-initiated access by a person employing a remote access client.” May need to work the definition to address non-traditional remote access methods that people might not recognize. The requirement does not specify what you’re accessing with IRA.

- Part 2.2: Lack of definition of confidentiality and integrity could lead to inconsistency of interpretation and implementation. Consider adding more clarity to the requirement language.
- Part 2.4: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?
- Part 2.5: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?
- Part 2.6: Please clarify why storage was not included in the requirement scope. In reading this, it appears that an Intermediate System can now be in the same ESP or ESZ as the BES Cyber Systems they are protecting. Is this intentional? In addition, significant architectural work may be required by some entities to comply with this.

Likes 0

Dislikes 0

Response

Quintin Lee - Eversource Energy - 1,3

Answer	No
Document Name	

Comment

While Eversource supports the recommendations made by the V5TAG to include dial-up connectivity whenever such connectivity is used for Interactive Remote Access, we do not support the use of the proposed new terms ESZ and SCI as discussed in our response to Question 1.

Likes 0

Dislikes 0

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	No
Document Name	

Comment

The Exelon companies agree with the comments submitted by EEI.

Likes 0

Dislikes 0

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
CHPD agrees with the changes proposed for R2.1, R2.2, R2.3, R2.4, and R2.5. CHPD does not agree with the inclusion of language in R2.6. The proposed R2.6 language to require CPU and memory to be shared only with other VCA Intermediate Systems discourages virtualization of Intermediate Systems. CHPD recommends removing “may only share CPU, memory” from the requirement language, but agrees that dedicating an ESZ/ESP to Intermediate Systems is appropriate.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
There is little risk difference between “Interactive” remote access and “System-to-System” remote access. In either case, strong methods of authentication, integrity, and non-repudiation controls are highly advisable. The concept of a real-time “live hack” popularized by movie “hackers” is generally a fallacy while in reality it requires highly coordinated scripting activities that leverage compromised trusted systems to execute exploits that are pre-staged by the threat actor. The benefit of the doubt that current CIP standards extend to supposedly trusted system-to-system communications is misplaced.	
Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

There is inconsistency between Requirement, R2 Part 2.1 and Requirement, R2 Part 2.6. Requirement R2, Part 2.1 is to, “Ensure that Interactive Remote Access is through an Intermediate System that is not inside an applicable ESP or ESZ” and R2 Part 2.6 requirement is, “IS may only share CPU, memory, or ESZ or ESP with other IS”. So, an Intermediate System must be outside an ESP or ESZ, per Requirement, R2.1, therefore, Requirement, R2.6 should be revised as follows: “Intermediate Systems can only share CPU and memory with other Intermediate Systems”.

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3,5

Answer	No
Document Name	

Comment

AEP is unable to agree with the proposed modifications to CIP-005 R2 at this time due to the need for clarity around some of the new proposed terms. Please see AEP’s response to Question #1.

Likes 0	
Dislikes 0	

Response

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO

Answer	No
Document Name	

Comment

We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

We cannot agree until the concerns posed in Questions 1 thru 8 are addressed.

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

Oncor supports EEI's comment.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

SWG offers the following items for consideration.

- R2: The leading requirement could use revision to be clearer. Consider, “Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R2 –Remote Access Management,* per system capability.” The remaining language should be addressed in the applicability or requirement language in the table.
- Part 2.1: Consider “User-initiated access by a person employing a remote access client.” May need to work the definition to address non-traditional remote access methods that people might not recognize. The requirement does not specify what you accessing with IRA.
- Part 2.2: Lack of definition of confidentiality and integrity could lead to inconsistency of interpretation and implementation. Consider adding more clarity to the requirement language.

- Part 2.4: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?
- Part 2.5: Should this include all EACS and PACS to align to the FERC direction of future supply chain modifications?
- Part 2.6: Please clarify why storage was not included in the requirement scope. In reading this, it appears that an Intermediate System can now be in the same ESP or ESZ as the BES Cyber Systems they are protecting. Is this intentional? In addition, significant architectural work may be required by some entities to comply with this.

Likes 0	
Dislikes 0	

Response

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

See EEI Comments.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF

Answer	No
Document Name	

Comment

All CIP standards impacted by virtualization should be updated concurrently. The efforts for the entities to adopt these changes would be significant.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the modifications on the removal of the prescriptive language in Part 2.2, making it more objective-based, and the enhanced security due to the Interactive Remote Access definition modifications which would now cover serial and dial-up connectivity.	
Likes 0	
Dislikes 0	
Response	
Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
City Light generally supports the proposed R2 modifications, with the exception of scope change as discussed above under Question 8, and the overarching concerns discussed in Questions 1 and 13.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1,3,5	
Answer	Yes
Document Name	
Comment	
There should be considerations for all CIP standards impacted by virtualization be updated concurrently to ensure efforts to make the necessary modifications to existing architecture by the entity.	

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource

Answer	Yes
Document Name	

Comment

R2 – the new Requirement remove the need for a mitigation plan. The Entity only needs to provide evidence the system is not capable. While we agree with intent of removing TFEs, we suggest these new words are less secure.

Part 2.1 – request clarification. How are TCAs covered?

Part 2.3 – for improved comprehension, we suggest that Part 2.3 borrow these words from Part 2.2 – “between the client and the Intermediate System”

Part 2.6 – request clarification. We believe the Requirement wants to say that the Intermediate Systems and the BES Cyber Systems must be on different virtual machine hosts.

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Neil Swearingen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment
Part 2.1 - The proposed language in R1.1 states “All applicable systems shall reside within one or more defined ESPs or ESZs. The applicable systems are listed as: High Impact BES Cyber Systems and their associated: PCA SCI PACS hosted on SCI EACS hosted on SCI And Medium Impact BES Cyber Systems connected to a network via routable protocol and their associated: PCA SCI PACS hosted on SCI EACS hosted on SCI Texas RE agrees with the language of this requirement. The requirement, however, is potentially problematic when combined with the language in R2.1 which states “Ensure that Interactive Remote Access is through an Intermediate System that is not inside an applicable ESP or ESZ.” Some entities choose to host their Intermediate Systems on Virtual Cyber Assets. An Intermediate System will meet the definition of EACS. For those Intermediate Systems that are virtualized they will meet the definition of EACS hosted on SCI. R1.1 requires that EACS hosted on SCI reside within one or more defined ESPs or ESZs. R2.1 requires that an IS used for IRA is not inside an applicable ESP or ESZ. At best, this is a clarity issue where it is not immediately obvious that the ESP or ESZ the Intermediate System is residing within is not an “applicable” ESP or ESZ. At worst, this causes a scenario where the only acceptable Intermediate System is one that is not virtualized. Texas RE does not believe this is the SDT's intent. To address this, Texas RE proposes that the verbiage “that is not inside an applicable ESP or ESZ” be removed from R2.1. R2.1 would then read as “Ensure that Interactive Remote Access is through an Intermediate System.” The proposed language in R2.6, “IS may only share CPU, memory, or ESZ or ESP with other IS.”, would ensure the intention behind “that is not inside an applicable ESP or ESZ” in R2.1 is still being met. **Part 2.2** - The addition of “confidentiality and integrity” is an improvement over using just the word “encryption”. Encryption may provide confidentially but not integrity. For example, encryption with digital signatures would provide both. Texas RE recommends the language to be modified to “*For all*

Interactive Remote Access sessions, protect the confidentiality and integrity by utilizing encryption that terminates at an Intermediate System” or similar language.

The Technical Rationale states the following in regards to R2.2: the language “Protect the confidentiality and integrity of Interactive Remote Access between the client and the Intermediate System” prevents outdated encryption methods from being utilized. Texas RE disagrees that this requirement language prevents the use of outdated encryption methods. Outdated encryption methods provide more than zero protection and therefore would meet the language in this requirement.

Alternatively, if the language in this requirement is determined to allow the CEAs the judgement on whether or not a specific encryption technology is “good enough” this can lead to inconsistent enforcement across the regions.

Texas RE proposes that the SDT define a new term, Strong Encryption Standard. Strong Encryption Standard would be defined as “An Encryption Standard with a security strength of 112 bits or higher.” 112 bits was chosen as that is the minimum encryption strength permitted under NIST SP 800-175B, Section 3.4. As NIST deprecates weaker key strengths the expectation is the SDT would update the definition of Strong Encryption Standard to match the minimum strength recommended by NIST.

In addition to this new term, a new requirement would be drafted, similar in nature to CIP-007-6 R3.3.

R# - For the protections implemented in Part 2.2 that use encryption, use a Strong Encryption Standard.

This language would balance prescription with flexibility. CEAs would have a bright-line criteria to determine whether or not an encryption algorithm is acceptable to use, but at the same time registered entities would have the flexibility of choosing the encryption standard that is best for their environment. Texas RE recognizes that not all encryption algorithms are of equal strength, and some encryption algorithms may be insecure despite meeting the required 112 bit security strength. Texas RE would not be opposed to the SDT modifying the proposed definition of Strong Encryption Standard to include or reference a blacklist of encryption algorithms that are not acceptable to be used, but this may be overly burdensome for the amount of benefit it provides.

Part 2.3 – While it does not object to the proposed language in Part 2.3, Texas RE notes that the proposed language in R2.3 may have unintended consequences that drive a certain architecture type. A number of entities use multiple systems in order to comply with this requirement. For example, an entity may normally be blocked from remotely accessing their Intermediate System. The entity logs into a separate system using multi-factor authentication and they are now allowed to remotely access the Intermediate System.

Under that architecture, if the separate system is unavailable, the entity can still make use of the Intermediate System by physically accessing the Intermediate System and remotely accessing their applicable BCS (this is possible because the current IRA definition excludes remote access that originates from an Intermediate System).

Under the proposed language in R2 and R2.3 entities would be required to use multi-factor authentication when directly accessing the Intermediate System if they intend to use the Intermediate System to remotely access an applicable system from R2.1. This provides an overall improvement to security, but does introduce compliance risk if the Intermediate System is needed when MFA is unavailable.

Part 2.6 - Texas RE notes that the existing definition of ESP “The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.” and the proposed verbiage in requirement R2.6 “IS may only share CPU, memory, or ESZ or ESP with other IS” means that it is not possible for an Intermediate System to be located within an ESP. An Intermediate System is an EACS. If the “ESP” is only allowed to be populated with other EACS then the network will not contain any BCS. If the “ESP” does not contain any BCS then the “ESP” does not actually meet the definition of ESP. If the SDT intends to allow Intermediate Systems to be located within ESPs then the definition of ESP or the verbiage in R2.6 will need to be modified. Texas RE recommends modifying the definition of ESP to no longer include BCS as a scoping mechanism or to explicitly state that Intermediate Systems must be located within an ESZ. As Intermediate Systems are currently forbidden from being located within an ESP, explicitly requiring the Intermediate System to be located within a defined ESZ will achieve the SDT’s goal while having a minimal impact on registered entities. This, combined with R2.6’s requirement that Intermediate Systems can only share ESZ with other Intermediate Systems would ensure that the Intermediate Systems are both isolated and protected.

Texas RE notes that on page 36 of the Technical Rationale, there are extra bullet points in Parts 2.4 and 2.5, Applicable Systems column.

Likes 0	
Dislikes 0	

Response

11. Backwards Compatibility: What level of effort is required to migrate from existing definitions to new definitions on existing virtualized architecture?

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE does not have comments on this question.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	
Document Name	

Comment

The level of effort can be greatly reduced if “or ESP” is removed from the SCI definition and from the Requirements of R1.6. Including ESPs poses a backwards compatibility challenge; see Question 2 response.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer	
Document Name	

Comment

GSOC/OPC is supportive of making modifications to enable the standards to progress to a more technology agnostic model. To facilitate this transition, an implementation period of at least 24 months is recommended to ensure that these changes related to virtualization can be implemented efficiently and effectively. However, GSOC supports a more rapid pace for the revisions associated with the splitting of the PACS/PAMS and EAMS/EACS definitions as it is currently prohibiting the adoption of controls that would increase the security of BCAs and prompt adoption would foster overall security.

Likes 0	

Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1,5	
Answer	
Document Name	
Comment	
Fairly significant as almost every internal process will need modification	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1,3,5,6	
Answer	
Document Name	
Comment	
We disagree with all new definitions since they all can be covered by the current definitions.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	

Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
The level of effort required to accommodate these changes could be significant, but could be lessened by consideration of proposed changes provided in our responses to previous questions.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	
Document Name	
Comment	
The effort to the proposed changes without any modification are high because of virtualized PACS and EACS being brought into scope even if they don't share SCI with HIBCS or MIBCS. The IRA revisions also require more time to determine the impacts as the webinar added a twist with the revelation that the IP to serial conversion was in scope.	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6

Answer	
Document Name	

Comment

There will be some effort for our current architecture, since we are already utilizing virtualization. However, the level of effort necessary to develop plans, policies, procedures, and to document their application under revised CIP Standards, would be substantial. Although not as extensive as that required for the CIP v5 transition, utilities seeking to utilize virtualization in their BCS environments will need be prepared for a major effort to revise and validate their suite of CIP compliance policies, procedures, and document.

Likes 0	
Dislikes 0	

Response

Scott Langston - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5

Answer	
Document Name	

Comment

N/A - no existing virtualized architecture.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	
Document Name	

Comment

Each change to a standard creates additional work for an entity to evaluate its processes, revise where appropriate, implement the changes, and retrain employees, which is not cost-effective. The proposed changes to the CIP standards will have significant impacts on entities and will require substantial resources to implement. The proposed changes go beyond simply updating technology and/or documentation; they constitute a culture shift comparable to the CIP v5 transition. Entities must implement processes to achieve an understanding of new terms, buy in to their use, and change the culture to employ new terms. Entities must be provided enough time to determine the effects of the revised requirements and definitions, develop adequate processes, and train personnel appropriately to implement quality practices that improve BES reliability.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	
Document Name	

Comment

Very little effort to migrate.

Likes 0	
Dislikes 0	

Response

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC

Answer	
Document Name	

Comment

See EEI Comments.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	
Document Name	

Comment

Minimal work will be required for our existing environment to document compliance for the R1.6; however, if we choose to implement virtual firewalls, there will be additional work required to implement the changes and document compliance.

Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
SWG Comment: New definitions do not pose significant issue. Implementation of CIP-005 may pose issues with entities who must re-architect virtual infrastructure to meet the new verbiage. This is no small task and should be allowed adequate time.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	
Document Name	
Comment	
Based on preliminary assessment, the level of effort required is moderate. However, additional guidance on implementation and audit approach is needed in order to make a full evaluation.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	
Document Name	
Comment	
The effort appearss to be substantial; therefore, adequate time should be allowed to adapt a new architecture landscape.	
Likes 0	

Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The level of effort can be greatly reduced if “or ESP” is removed from the SCI definition and from the Requirements of R1.6. Including ESPs poses a backwards compatibility challenge; see Question 2 response.	
Likes 0	
Dislikes 0	
Response	
Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	
Document Name	
Comment	
The level of effort can be greatly reduced if “or ESP” is removed from the SCI definition and from the Requirements of R1.6. Including ESPs poses a backwards compatibility challenge; see Question 2 response.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	
Document Name	
Comment	
AEP is of the opinion that the effort required would be considerably high. It is difficult to say, however, without clarification of the ESZ definition.	
Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	
Document Name	

Comment

The level of effort is significant with backwards compatibility even if little or no virtualization is in use, because all processes must be reviewed and updated to accommodate current and future (inevitable) use of virtual systems.

CenterPoint Energy analyzed the project just for the High Impact BES Cyber Systems with the assumption of having existing staff (that are already tasked with other duties) dedicate 3 hours per day to the effort. Based upon this assumption and the time estimates for the associated tasks, this project will take two experienced analysts more than two years to complete the work.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	
Document Name	

Comment

To the extent an entity leverages new technologies the effort may be high.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

BPA believes the SDT has done an admirable job of preserving nested capabilities and backwards compatibility. While it will entail significant effort to migrate, it is justifiable effort.

Likes 0	

Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	
Document Name	
Comment	
CHPD believes that this language requires a significant amount of effort due to the lack of specific BCA scoping language in the SCI definition. Migrating to this language, as written, would require CHPD to classify additional Cyber Assets that perform no BES functions.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource	
Answer	
Document Name	
Comment	
There should be full compatibility that the existing CIP terminology and definitions should be acceptable going forward.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	
Comment	
The level of effort can be greatly reduced if “or ESP” is removed from the SCI definition and from the Requirements of R1.6. Including ESPs poses a backwards compatibility challenge; see Question 2 response.	
Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	
Document Name	

Comment

As we understand the redefinition, little to no effort will be required to maintain the existing paradigm. However, this will require a major effort to rearchitect the interaction between the devices and defining the policies that would supersede the existing ACLs that currently permit or restrict traffic to a policy-based system. Any migration will best be implemented in conjunction with a major system overhaul/refresh.

Will Entities be provided a phased in consideration for existing architecture and the implantation guidelines be reflective of the phased in approach?

Likes 0	
Dislikes 0	

Response

Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6

Answer	
Document Name	

Comment

While the changes are intended to allow for backward compatibility for currently implemented technology a significant effort is still needed for process/program updates as well as asset assessment procedures and device classification methods in order to adopt the new definitions. This effort should not be overlooked when pinpointing the implementation timeline for these new changes.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	
Document Name	

Comment

The Exelon companies agree with the comments submitted by EEI that while the effort appears to be substantial, the clarification of ESZ may lessen the effort.

Likes 0	
Dislikes 0	

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	
Document Name	

Comment

City Light considers that the level of effort would be mixed, with minimal to moderate effort on the technical side and extensive effort on the compliance and documentation side.

Minimal effort would be required for existing BES Cyber Systems themselves. There would likely be marginally additional level of effort required for designing and deploying the upgrade of BES Cyber Systems planned for calendar year 2020 and beyond. Beyond that, any additional technical effort brought about by upgrading to a virtualized architecture likely would be negligible.

However, the level of effort necessary to develop plans, policies, procedures, and to document their application under revised CIP Standards, would be substantial. Although not as extensive as that required for the CIP v5 transition, utilities seeking to utilize virtualization in their BCS environments—and that would be almost all of them—will need be prepared for a major effort to revise and validate their suite of CIP compliance policies, procedures, and documents. City Light anticipates that such an effort (for virtualization throughout all applicable CIP Standards) could require about a year of dedicated effort. Significant expense likely also would be incurred for external consultant support.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	
Document Name	

Comment

Overall, we believe that migrating from existing definitions to a majority of the new definitions in existing virtualized and non-virtualized environments will require a small amount of effort. However, we do feel that the term “Shared Cyber Infrastructure” and how the requirements are applied to those assets, will require a significant amount of work.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1,3

Answer

Document Name

Comment

Definitely impactful but not substantial.

See Eversource response to Question 7.

Likes 0

Dislikes 0

Response

Neil Swearingen - Salt River Project - 1,3,5,6 - WECC

Answer

Document Name

Comment

Based on the current budget/costs/resources for our High Impact Control Centers, the level of effort involved in a developing new processes, design/modification of network architecture, and the research and development needed in order to support new tools - 36 months or more would be needed.

Likes 0

Dislikes 0

Response

James Brown - California ISO - 2 - WECC

Answer

Document Name

Comment

New definitions do not pose significant issue. Implementation of CIP-005 may pose issues with entities who must re-architect virtual infrastructure to meet the new verbiage. This is no small task and adequate time should be allowed.

Likes 0

Dislikes 0

Response

Michael Puscas - ISO New England, Inc. - 2	
Answer	
Document Name	
Comment	
The effort required would be very significant because in several instances there is no backwards compatibility.	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5	
Answer	
Document Name	
Comment	
SDG&E supports EEI's comments submitted on our behalf.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy	
Answer	
Document Name	
Comment	
Duke Energy is currently assessing the impact of migrating from the existing definition to the new definition on existing virtualized architecture.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL	

Answer	
Document Name	
Comment	
Westar / Kansas City Power & Light support Edison Electric Institute's (EEI) response to Question 11.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	
Document Name	
Comment	
LAK believes that the actual question is not just the level of effort to migrate from existing to new definitions for backwards compatibility. For entities who need to maintain the existing terms and moving toward new definitions, they will likely need to address their entire CIP program, from start to finish. Even adopting the new terms and new requirements as entities move toward more virtualization will require updates to CIP-002 programs to ensure that the devices are identified and categorized appropriately. The new requirements (not just for CIP-005, but the conforming changes and nuances of the changes to the standards based on new and revised glossary terms) will be just as dramatic to implement as CIP Version 5. While LAK believes that it is the right way to go, LAK has concerns that it will take considerable effort, both in terms of time and energy as well as in dollars, to implement. We do not believe that industry will be able to adopt it and incorporate the new definitions and changes to a single set of the CIP suite of standards such as CIP-005-6 without overhauling the entire CIP program (including training and security awareness as well as the more technical security based standards)	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
The effort appears to be substantial; however, with the clarification of ESZ, it may help lessen the effort.	
Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer	
Document Name	

Comment

MISO Comment: The proposed new definitions on existing virtualized architecture do not pose any significant issues. In contrast, CIP-005-7 as currently written is not directly Backwards Compatible and, as such, has the potential to pose significant issues for entities who must re-architect virtual infrastructure to comply with the new verbiage. For this reason, MISO recommends the Implementation Plan for CIP-005-7 allow adequate time for entities to come into compliance with the new standard; i.e. 36 months.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 1,3,6

Answer	
Document Name	

Comment

In our transmission operations control centers we are removing all Virtual infrastructure so effort would be non-existent. However, for our RSA and AMAG these will need to be relocated to an ESP and split into two sets of systems for Medium and High sites.

This will be a very low to low effort for our generation fleet.

Likes 0	
Dislikes 0	

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer	
Document Name	

Comment

Significant level of effort due to issues with inclusion of serial connectivity. As previously stated in the answer to question #2, we may need additional hardware/infrastructure to comply with the current draft.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC

Answer	
Document Name	

Comment

PG&E indicates the following:

1 – For CIP-002, PG&E does not foresee any backward compatibility issues since virtualization is currently lightly used. It does appear the effort to record the new Cyber Asset types (i.e. EACS, EAMS, PAMS, VCA, etc..) will require internal process modifications and some yet to be determined administrative effort to verify they are identified and documented as virtualization is expanded.

2 – For CIP-005, similar to the above CIP-002 input, PG&E does not foresee any backward compatibility issues since virtualization is currently lightly used within the BCS environment. There is a concern about the creation of the proper documentation to demonstrate compliance with the different connectivity/communication methods to be allowed. With the expansion of definitions and potential methods to meet the protection objectives, it is very possible evidence can be created that an Audit Team would deem insufficient. This is especially true for some of the newer technology that Audit Teams do not have experience with.

Recommendation - PG&E recommends the SDT work on guidance for the generation of proper evidence to help reduce differences in interruption.

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name Aubrey Short, On Behalf of:

Answer	
Document Name	

Comment

The document has made significant effort to maintain compatibility with CIP-005-6.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	
Document Name	
Comment	
GTC is supportive of making modifications to its program in order for the standards to progress to a more technology agnostic model. We recommend that at least 24 months be permitted to make these changes related to virtualization. However, we also request that the splitting of the EAMS and EACS definition occur promptly as it is currently prohibiting the adoption of controls that would increase the security of BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	
Document Name	
Comment	
N&ST believes the SDT’s efforts to maintain “backward compatibility” that will not force entities with existing, non-virtualized environments to make any significant changes have been largely successful. N&ST believes the impact on entities that are presently utilizing highly virtualized networking and computing environments could, depending on their detailed configurations, range from minor to fairly significant.	
Likes 0	
Dislikes 0	
Response	

12. The SDT posted a draft CIP-005-7 Technical Rationale document to explain the basis behind these proposed changes. Please provide any additional comments on this document

Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF	
Answer	
Document Name	
Comment	
Alliant supports MRO NSRF's comments.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	
Document Name	
Comment	
Most of our comments are addressed in other comments. The rationale does not appear to have any outstanding errors, but most of the focus was on the actual requirements. The rationale will need to be revised if modifications are made.	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer

Document Name

Comment

Southern applauds the SDT for the hard work in the development of the draft CIP-005-7 Technical Rationale document that provides thorough descriptions of the proposed changes and visual organization of these newly proposed concepts. Additional clarification on new Glossary Terms and revisions to existing terms will help bring the industry closer to continued forward progress towards enhanced security and reliability through these new risk-based approaches.

Likes 0

Dislikes 0

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer

Document Name

Comment

None.

Likes 0

Dislikes 0

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer

Document Name

Comment

In our view, if all virtual devices are identified properly, they will fall within the definition of BCA, EACMS, or PACS, the logical isolation may not be needed since all CIP Cyber Asset are protected by the current CIP requirements.

Likes 0

Dislikes 0

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer

Document Name

Comment

None.

Likes 0

Dislikes 0

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer

Document Name

Comment

GSOC/OPC requests additional clarity regarding the intent of the last paragraph on p. 26 of the Technical Rationale document relative to the explanation of the interaction between CIP-012 and CIP-005 super-ESP concept.

Likes 0

Dislikes 0

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer

Document Name

Comment

We agree with EEI's comments and appreciate the hard work done by the SDT in the development of the draft CIP-005-7 Technical Rationale document believing that it provides a thorough description of the proposed changes.

If the SDT should decide to revise the document, we would request enlargement of the diagrams on pp. 20-21, additional annotation of the components, and color coding of the lines with respect to serial and routable protocol for greater clarity.

To help entities interpret the diagrams for their systems, the location Alpha scenarios should be updated to show the following:

A single unit for a plant DCS system – where the system could be local routable with serial conversion then out, or routable end to end

Substations where the end point devices are serial connected BCS (all diagrams depict blue-line connectivity that implies local routable connectivity – this could be true with some systems in the substations)

Provide clarity where a “protocol break” vs IP to serial conversion pass-through occurs in the diagrams. Previous guidance suggests that this changes whether ERC exists or not.

The differences between High and Medium Impact applications

Make it clearer where “system-to-system” communications is occurring.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE included comments on the Technical Rationale in its answers to #9 and #10.

Likes 0	
Dislikes 0	

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer	
Document Name	

Comment

GTC requests additional clarity regarding the intent of the last paragraph on p. 26 of the Technical Rationale document relative to the explanation of the interaction between CIP-012 and CIP-005 super-ESP concept.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC

Answer

Document Name

Comment

PG&E indicates the Technical Rationale document does provide good information on the modifications and their impact. There is a great deal of information contained with the document which requires multiple readings and back-and-forth referencing between some sections to fully understand the impacts. PG&E believes the magnitude of the modifications necessitate the current condition of the document and does not have any recommendations for improvement in its presentation.

Recommendation - As noted in PG&E Question 2 input, we recommend if SCI of different impact ratings cannot share the same CPU and memory, it be clearly indicated within the Technical Rationale document.

Likes 0

Dislikes 0

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer

Document Name

Comment

The diagrams do not clearly depict the demarcation points between the hypervisors, management system and SCI. In addition, the diagrams do not provide examples where there is no separate management system and the built-in features of hypervisors are used to manage the SCI. In such scenarios, it appears that accessing the hypervisor directly would not comply with CIP-005-7 R1.6. Also, see Tri-State's other comments regarding defining management systems, management plane, data plane and providing examples.

On page 7 of the Technical Rationale, the sentence “The reliance on “using a routable protocol” has been removed to incorporate IP to serial conversion scenarios to serial only Cyber Assets” is inconsistent with the removal of ERC from the revised definition of IRA. The SDT could change it to: “If a serial is converted to IP before leaving the substation.”

Likes 0

Dislikes 0

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF

Answer

Document Name

Comment

None

Likes 0

Dislikes 0

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer

Document Name

Comment

EEI appreciates the hard work done by the SDT in the development of the draft CIP-005-7 Technical Rationale document, believing that it provides a thorough description of the proposed changes. However, EEI member companies recommend clarifying the new NERC Glossary Terms along with revisions to existing terms while not creating new compliance obligations for entities that do not use a virtualization.

Likes 0

Dislikes 0

Response

Patricia Boody - Lakeland Electric - 1,3,5,6

Answer

Document Name

Comment

LAK believes that the Technical Rationale is a good start but may need additional explanations for some of the concepts (for example R Parts 2.4 and Part 2.5 related to system-to-system remote access). We appreciated the extension of time to review all documentation; however, other obligations prevented LAK from a detailed review of the TR document.

Likes 0

Dislikes 0

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer

Document Name

Comment

Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 12.

Likes 0

Dislikes 0

Response

Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy

Answer

Document Name

Comment

Duke Energy does not have any additional comments at this time.

Likes 0

Dislikes 0

Response

Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5

Answer

Document Name

Comment

SDG&E supports EEI’s comments submitted on our behalf.

Likes 0

Dislikes 0

Response

Michael Puscas - ISO New England, Inc. - 2

Answer

Document Name

Comment

The Technical Rationale goes further than the requirements. For example, the Technical Rational explains what “affinity” means, but that is not included in the requirements. Concepts such as “affinity” should be included in the requirements, not just in the Technical Rationale.

Likes 0

Dislikes 0

Response

James Brown - California ISO - 2 - WECC

Answer

Document Name

Comment

No additional comments on the technical rationale document.

Likes 0

Dislikes 0

Response

Neil Swearingen - Salt River Project - 1,3,5,6 - WECC

Answer

Document Name

Comment

SRP has no additional comments.

Likes 0

Dislikes 0

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer

Document Name

Comment

We appreciate the SDT’s work on this document. It provides valuable information and guidance to entities on the updated requirements.

Likes 0

Dislikes 0

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer	
Document Name	

Comment

Great job! City Light recognizes the hard work by the SDT and appreciates the effort to explain and clarify the proposed modifications.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	
Document Name	

Comment

The Exelon companies agree with the EEI recommendation to clarify the NERC Glossary Terms so as not create new compliance obligations for entities that do not use virtualization.

Likes 0	
Dislikes 0	

Response

Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6

Answer	
Document Name	

Comment

AZPS would like to see more explanation in the technical rational on how virtualized networking should be considered. Software defined networking needs more emphasis in the use with virtualized system. AZPS believes this is needed as we implement the zero trust security architecture in accordance with the CIP requirements.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	
Document Name	

Comment

Request for additional information to be contained in the Technical Rationale document are included in our response to previous questions.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

We agree with EEI comments and appreciate the hard work done by the SDT in the development of the draft CIP-005-7 Technical Rationale document believing that it provides a thorough description of the proposed changes.

If the SDT should decide to revise the document, we would request enlargement of the diagrams on pp. 20-21, additional annotation of the components, and color coding of the lines with respect to serial and routable protocol for greater clarity.

To help entities interpret the diagrams for their systems, the location Alpha scenarios should be updated to show the following:

A single unit for a plant DCS system – where the system could be local routable with serial conversion then out, or routable end to end

Substations where the end point devices are serial connected BCS (all diagrams depict blue-line connectivity that implies local routable connectivity – this could be true with some systems in the substations)

Provide clarity where a “protocol break” vs IP to serial conversion pass-through occurs in the diagrams. Previous guidance suggests that this changes whether ERC exists or not.

The differences between High and Medium Impact applications

Make it clearer where “system-to-system” communications is occurring.

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	
Document Name	
Comment	
CHPD believes that it would be useful to include examples of successful compliance of the proposed changes. The current wording makes it difficult to realize implementation of virtualized BES Cyber Systems in a mixed-trust environment. Examples should directly identify controls that can be applied to enable the use of CIP and non-CIP devices within the same virtual environment.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
BPA largely agrees with the Technical Rationale, and the case for virtualization changes is supported by literally incalculable benefit. The TR does a good job with the basics; there is justification far beyond what can be captured in a single white paper or on this comment form.	
Likes 0	
Dislikes 0	
Response	
Kent Feliks - AEP - 3,5	
Answer	
Document Name	
Comment	
AEP is appreciative of the efforts of the SDT in not only the standard modifications but also the Technical Rationale document. We also recommend providing some clarification surrounding the ESZ definition as well as ensuring new compliance obligations are not created for those who do not use virtualization currently.	
Likes 0	
Dislikes 0	
Response	

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO	
Answer	
Document Name	
Comment	

We agree with EEI comments.

EEI appreciates the hard work done by the SDT in the development of the draft CIP-005-7 Technical Rationale document believing that it provides a thorough description of the proposed changes.

If the SDT should decide to revise the document, we would request enlargement of the diagrams on pp. 20-21, additional annotation of the components, and color coding of the lines with respect to serial and routable protocol for greater clarity.

To help entities interpret the diagrams for their systems, the location Alpha scenarios should be updated to show the following:

A single unit for a plant DCS system – where the system could be local routable with serial conversion then out, or routable end to end

Substations where the end point devices are serial connected BCS (all diagrams depict blue-line connectivity that implies local routable connectivity – this could be true with some systems in the substations)

Provide clarity where a "protocol break" vs IP to serial conversion pass-through occurs in the diagrams. Previous guidance suggests that this changes whether ERC exists or not.

The differences between High and Medium Impact applications

Make it clearer where "system-to-system" communications is occurring.

Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	

We agree with EEI comments.

EEI appreciates the hard work done by the SDT in the development of the draft CIP-005-7 Technical Rationale document believing that it provides a thorough description of the proposed changes.

If the SDT should decide to revise the document, we would request enlargement of the diagrams on pp. 20-21, additional annotation of the components, and color coding of the lines with respect to serial and routable protocol for greater clarity.

To help entities interpret the diagrams for their systems, the location Alpha scenarios should be updated to show the following:

A single unit for a plant DCS system – where the system could be local routable with serial conversion then out, or routable end to end

Substations where the end point devices are serial connected BCS (all diagrams depict blue-line connectivity that implies local routable connectivity – this could be true with some systems in the substations)

Provide clarity where a “protocol break” vs IP to serial conversion pass-through occurs in the diagrams. Previous guidance suggests that this changes whether ERC exists or not.

The differences between High and Medium Impact applications

Make it clearer where “system-to-system” communications is occurring.

Likes 0	
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	
Document Name	
Comment	
See EEI Comments.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	
Document Name	
Comment	
No Additional Comments.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	

Document Name	
Comment	
Reclamation appreciates the time and effort put into producing the CIP-005-7 Technical Rationale and believes it is a needed document to provide the framework for the revised CIP-005-7 standard.	
Likes 0	
Dislikes 0	
Response	

13. Provide any additional comments for the SDT to consider, if desired

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

In regards to filling out the evidence request spreadsheet, registered entities that are already implementing virtualization now must identify and adjust for new terms. Registered entities that are currently using virtualized environments list the host (hypervisor) as a CA (BCA, EACMS, PACS, PCA, etc.) and include the VMs.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	
Document Name	

Comment

We agree with EEI comments:

"EEI notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, EEI suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

For example: If you use virtual, then take path B; if not, continue with path A's existing requirements. We believe such an approach would provide an easier transition."

We submit as a possible solution to backwards compatibility the precedent established by the PRC-005-2 Implementation Plan, whereby an Entity could choose to remain compliant with PRC-005-1.1b on a component by component basis until it elected PRC-005-2, or was required to by the 100% compliance implementation date.

For CIP-005-7, the Implementation Plan could include language such as: "Each Responsible Entity shall maintain documentation to demonstrate compliance with either CIP-005-6 (according to the Glossary Terms as defined prior to the conforming changes driven by CIP-005-7) or CIP-005-7 (or subsequent versions), but not both, for a given ESP or ESZ."

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 3,4

Answer

Document Name

Comment

GSOC/OPC is concerned that the list of Applicable Systems identified in Section 4 of CIP-005 is not reflective of the “systems” listed within the requirements table. The requirements table and Section 4 of the standard should reflect/list the same potential “Applicable Systems” as applicable across and within the standard. Accordingly, GSOC/OPC recommends that the SDT review this discrepancy and make the revisions necessary to ensure consistency.

Further, GSOC/OPC is concerned that some of the “systems” listed as “Applicable Systems” within the requirements table are not necessarily systems and, therefore, do not necessarily easily lend themselves to identification of a particular asset or system. For this reason, such classification may result in each Responsible Entity attempting to “translate” such system into a set of associated assets, e.g., ESP and ESZ. Such translation could vary greatly by and amongst Responsible Entities as well as the ERO and its auditors. GSOC/OPC recommends that the SDT review these revisions to the “Applicable Systems” column to ensure that the objective and applicability is clear, unambiguous, and feasible.

GSOC/OPC notes that the use of terms versus associated acronyms is inconsistent in the proposed draft of CIP-005, e.g., use of “IS” versus use of “Intermediate System.” GSOC/OPC recommends the SDT evaluate the proposed draft for consistent usage of acronyms versus defined terms.

Finally, GSOC/OPC notes that there was not an update to or an indication of review of VSLs or VRFs. It is recommended that such review occur to ensure that they remain consistent with the requirements of CIP-005.

Likes 0

Dislikes 0

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5

Answer

Document Name

Comment

None.

Likes 0

Dislikes 0

Response

Bruce Reimer - Manitoba Hydro - 1,3,5,6

Answer

Document Name

Comment

We disagree with the proposed changes. In our view, current CIP requirements can apply to virtualization environment smoothly without significant changes. Given that the CIP compliance program today works fairly smoothly by implementing the existing requirements, any changes of requirements and definitions beyond virtualization shouldn’t be targeted such as network layer protection for EACMS and PACS proposed in CIP-005-7 R1. SDT should focus on how to resolve CIP compliance in the virtualization environment without prohibiting the new technology rather than try to change the requirements for the defense in depth since it is not the driver for this project. Resulting from our comments in the above questions, as long as the Cyber Asset definition are modified to include virtual devices, most of existing CIP V5 requirements would apply to virtualization environment seamlessly.

Likes 0

Dislikes 0

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer

Document Name

Comment

Xcel Energy supports the comments of Edison Electric Institute.

Likes 0

Dislikes 0

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer

Document Name

Comment

The new CIP-005 standard provides more clarity around the use of virtual infrastructure and virtual machines, but will require 2-3 years for some companies to implement – this is not a like to like change.

ERCOT suggests spelling out acronyms in all requirement parts in order to ensure they are clearly understood.

Removable Media: Examples were removed. However, examples were still listed for Transient Cyber Asset. ERCOT believes Examples are very helpful.

PAMS and PACS: Based on the implementations, mounted hardware or devices might not actually be mounted exactly at the Physical Security Perimeter. ERCOT suggests the SDT consider rewording.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	
Document Name	

Comment

SDT needs to remember that some technologies are not virtualization specific. The idea of an ESZ and policies can apply to physical systems today. Windows has Windows Firewall and Group Policy can push out policies for those host-based firewalls. This means an operator workstation with a Window Firewall enabled could be a BCA and EACS and SCI under the proposed definitions. Those workstations also have a single network address but across usually two NICS. If that is the case then under proposed CIP-005 R1.6 what is the management system for that operator workstation? If it is the same NICS used for SCADA and other typical operations tasks then there can be no separation of that management plane.

Some of the new requirements still have a prescriptive rather than objective bent. Please try to word the requirements to give entities an objective to met rather than the SDT determine the risk and prescribe the solution. Instead define the risk and the objective regarding the risk. This is what we attempted to do in comment #5, “Have a means to reduce risk of a VCA utilizing CPU, memory, or storage in a way that prevents other VCAs from having access to those resources.”

Again we understand the effort the SDT has put into this and this is not an easy task. We hope the comments help the SDT towards its goals of more objective rather than prescriptive requirements that addresses all the items before the SDT.

Likes 0	
Dislikes 0	

Response

Jenifer Holmes - Alliant Energy Corporation Services, Inc. - 4 - MRO,RF

Answer	
Document Name	

Comment

Alliant supports MRO NSRF's comments.

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1,3,5,6

Answer

Document Name

Comment

No additional comments

Likes 0

Dislikes 0

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer

Document Name

Comment

Reclamation recommends that electronic isolation distinguish between system protection levels along with BES and non-BES. An Electronic Security Zone (ESZ) could become a risk to BES Cyber Systems when stretched to corporate business enclaves through virtual machine hyper jumping from a lower trust business network. Mixed trust environments on shared infrastructure between CIP Applicable Systems and corporate business networks could also introduce unnecessary risk to the BES. All shared infrastructure needs to be protected at the highest level of identified system that resides on it.

Likes 0

Dislikes 0

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer

Document Name

Comment	
None	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	
Document Name	
Comment	
See EEI Comments. Also, the language used in the CIP-005-7 R1.6 and R2.6 requirements is confusing. The use of multiple "or" statements makes the requirements difficult to interpret. Also, the term "management plane" is not defined, but is referenced twice in the standard.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	

Document Name

Comment

The new CIP-005 standard provides more clarity around use of virtual infrastructure and virtual machines but will require 2-3 years for some companies to implement – this is not a like to like change. It is somewhat noteworthy that many entities have already implemented virtual infrastructure and are able to comply, even under audit scrutiny, to the current wording of the standards. As such, the SWG believes current approved and implemented versions of the standards allow and support virtualization with no change.

General comment: Spell out acronyms in all requirement parts to ensure clear understanding.

Removable Media: Examples were removed. However, examples were still listed for Transient Cyber Asset. Examples are very helpful.

PAMS and PACS: Based on the implementations, mounted hardware or devices might not actually be mounted exactly at the Physical Security Perimeter. Consider rewording this.

Likes 0

Dislikes 0

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6

Answer

Document Name

Comment

No additional comments.

Likes 0

Dislikes 0

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer

Document Name

Comment

We agree with EEI comments:

“EEI notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, EEI suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

For example: If you use virtual, then take path B; if not, continue with path A’s existing requirements. We believe such an approach would provide an easier transition.”

We submit as a possible solution to backwards compatibility the precedent established by the PRC-005-2 Implementation Plan, whereby an Entity could choose to remain compliant with PRC-005-1.1b on a component by component basis until it elected PRC-005-2, or was required to by the 100% compliance implementation date.

For CIP-005-7, the Implementation Plan could include language such as: “Each Responsible Entity shall maintain documentation to demonstrate compliance with either CIP-005-6 (according to the Glossary Terms as defined prior to the conforming changes driven by CIP-005-7) or CIP-005-7 (or subsequent versions), but not both, for a given ESP or ESZ.”

Likes 0	
Dislikes 0	

Response

Andy Crooks - SaskPower - 1,3,5,6,9 - MRO

Answer	
Document Name	

Comment

We agree with EEI comments:

“EEI notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, EEI suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

For example: If you use virtual, then take path B; if not, continue with path A’s existing requirements. We believe such an approach would provide an easier transition.”

We submit as a possible solution to backwards compatibility the precedent established by the PRC-005-2 Implementation Plan, whereby an Entity could choose to remain compliant with PRC-005-1.1b on a component by component basis until it elected PRC-005-2, or was required to by the 100% compliance implementation date.

For CIP-005-7, the Implementation Plan could include language such as: “Each Responsible Entity shall maintain documentation to demonstrate compliance with either CIP-005-6 (according to the Glossary Terms as defined prior to the conforming changes driven by CIP-005-7) or CIP-005-7 (or subsequent versions), but not both, for a given ESP or ESZ.”

Likes 0	
Dislikes 0	

Response

Kent Feliks - AEP - 3,5

Answer	

Document Name	
Comment	
Many improvements made in this proposal are noted over the previous version. However, the proposed terms and requirement modifications need some clarification. AEP suggests taking an approach to these modifications that involves offering alternatives to virtualization within the standard. We understand it can be difficult to provide a new path for virtualization while also maintaining existing requirements, but we feel that both are needed.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Public Utility District No. 1 of Chelan County	
Answer	
Document Name	
Comment	
CHPD believes that it would be useful to see how these proposed changes are going to be applied to the other standards, particularly CIP-007 and CIP-010. It is difficult to identify how our existing workflows will change under the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	

Document Name	

Comment

As mentioned above, the proposed changes will bring auditing challenges for auditors as each policy based environment vendor will have differing approaches as well as modules, tools, monitoring, etc. to present policies versus existing environments with firewalls which can be presented uniformly (source, destination, port). We feel prior to approval(s), a standardized and approved audit approach should be published to the industry for auditing policy based environments.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no NGrid and Eversource

Answer	
Document Name	

Comment

Comments on the Definitions

Shared Cyber Infrastructure (SCI) - we recommend changing from “Programmable electronic devices whose compute, storage” to “Programmable electronic devices whose processing resources”

Transient Cyber Asset (TCA)

- Should some TCA/VCA (Virtual Cyber Asset) be considered BCA (BES Cyber Asset)?
- We request a use case to better understand this standardized configuration
- Request clarification. Since the TCA needs to connect to a SCI, that forces the SCI to comply. What does the SCI comply with?

Protected Cyber Asset (PCA) – request confirmation that “shared compute resources” means other virtualized instances on the same SCI hypervisor

EACS (Electronic Access Control System) & EAMS (Electronic Access Monitoring System) – we request keeping the old term / definition / applicability EACMS in addition to these two new terms / definitions / applicability. We suggest that the Entity has the flexibility to use any of these three terms / definitions / applicability to avoid forcing Entities in to costly, large changes to their documentation and training, etc.

ESZ (Electronic Security Zone) – we recommend changing from “A segmented section of a network that contains systems and components to create a logical isolation” to “is a network that is logically isolated” because the network is logically isolated, a segment is not. The network does not “contain systems and components to create a logical isolation.”

PSP (Physical Security Perimeter) – we recommend changing from “The physical border at which access is controlled.” to “The border at which physical access is controlled.”

Comments on the Standard – Exemptions

4.2.3 - request clarification. Will these Exemptions apply to all CIP Standards?

4.2.3.3 – request clarification since this new exemption is not consistent with CIP-006 R10 to physically protect communication lines between PSPs (Physical Security Perimeter)

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

We agree with EEI comments:

“EEI notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, EEI suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

guidance suggests that this changes whether ERC exists or not.

The differences between High and Medium Impact applications

Make it clearer where “system-to-system” communications is occurring.

Provide any additional comments for the SDT to consider, if desired.

Comments:

We agree with EEI comments:

“EEI notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, EEI suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

For example: If you use virtual, then take path B; if not, continue with path A’s existing requirements. We believe such an approach would provide an easier transition.”

We submit as a possible solution to backwards compatibility the precedent established by the PRC-005-2 Implementation Plan, whereby an Entity could choose to remain compliant with PRC-005-1.1b on a component by component basis until it elected PRC-005-2, or was required to by the 100% compliance implementation date.

For CIP-005-7, the Implementation Plan could include language such as: “Each Responsible Entity shall maintain documentation to demonstrate compliance with either CIP-005-6 (according to the Glossary Terms as defined prior to the conforming changes driven by CIP-005-7) or CIP-005-7 (or subsequent versions), but not both, for a given ESP or ESZ.”

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1,3,5

Answer	
Document Name	

Comment

There should be considerations for all CIP standards impacted by virtualization be updated concurrently to ensure efforts to make the necessary modifications to existing architecture by the entity. Additionaly, ensure all new terms are defined.

Likes 0	
Dislikes 0	

Response

Chinedu Ochonogor - APS - Arizona Public Service Co. - 1,3,5,6

Answer	
Document Name	

Comment

The full impact of the proposed definition changes is difficult to assess without also reviewing the proposed changes to CIP-007 and CIP-010. AZPS would like to have the ability to comment on these definition changes along with the CIP-007 and CIP-010 commenting periods. AZPS appreciates and supports the work invested in modifying these requirements. The transparent nature the SDT has taken to relay the intent and need for change has not gone unnoticed.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer

Document Name

Comment

Consider rewording CIP-005 R1 P1.6 and R2 P2.6 for better clarity.

Likes 0

Dislikes 0

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer

Document Name

Comment

The Exelon companies appreciate the opportunity to comment on this important topic and the good work being done by the SDT. We also however agree with the EEI comments expressing concern that absent additional clarification the proposed version may create unnecessary burden for registered entities that are not planning to deploy virtualization.

Likes 0

Dislikes 0

Response

Matthew Nutsch - Seattle City Light - 1,3,4,5,6 - WECC

Answer

Document Name

Comment

City Light again commends the SDT on their persistence and effort to tackle this tough challenge.

One gap that we would like to see addressed by the SDT is guidance to demonstrate consistency of the proposed virtualization modifications for High and Medium assets with use of virtualization at Low assets under CIP-003-7 R2 Attachment 1 Section 3 Electronic Security. As much as possible, please be sure the approaches proposed here do not directly conflict with the extensive guidance about electronic access provided to support CIP-003-7.

City Light also asks that any new security requirements for existing physical BCS and associated devices be removed from this proposed Standard and be discussed and balloted separately. To minimize scope creep, we request that the risks be quantified and presented that justify these expanded non-virtualization requirements, those that add new security controls beyond the conceptual changes necessary to accommodate virtualization in the CIP standards.

Likewise, City Light asks that other non-virtualization concepts, such as the changes to treatment of routable connectivity and Dial-up Connectivity be treated in a separate comment period and proposal. We appreciate the efforts of the SDT to identify the location and nature of non-virtualization changes in this material and comment form, but we feel all non-virtualization changes should be treated separately. The modifications for virtualization are a big enough lift on their own, they and should not be combined (and confused) with other unrelated changes.

City Light also recommends that the SDT strongly recommend that NERC conduct a pilot program to evaluate the CIP modifications for virtualization, because of the many changes and new definitions that are required in the existing Standards. Such a pilot program could be similar to the one conducted in all regions as part of (and prior to) the CIP v5 transition.

City Light requests that the phrase "that could lead to misoperation or instability in the BES" be restored to the Purpose statement of proposed CIP-005-7. This phrase is an essential scoping statement necessary to identify the applicability of the controls of CIP-005.

Finally, we note the incorrect punctuation for (presumably) the plural of acronyms as used throughout this comment form, the proposed CIP-005-7, and supporting materials. For instance, the plural of "VCA" is "VCAs," not "VCA's" as used above. "VCA's" is the possessive form, and by context that is not what is intended in the draft documents.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	
Document Name	

Comment

Overall, we support the updates to CIP-005. However, there are several instances where verbiage is focused almost solely on virtualization, and we see opportunities where entities might be confused as to whether it applies to existing, non-virtualized infrastructure and, if it does apply, confusion on how it would apply. Additionally, there appears to be a significant amount of change to documentation and evidence that will impact entities with no virtualized environment or virtualized environments that are segmented are in compliance today. While some of this might be unavoidable, it would be prudent of the SDT to continue to actively consider how to make updates to the standards without placing a large burden on entities that would like to "stay the way they are today."

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1,3

Answer	
Document Name	

Comment

Eversource notes many improvements over the previous virtualization proposal, however we remain concerned over the level of change to the CIP Standards: new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements. To address these concerns, Eversource suggests the SDT take another approach to virtualization by offering clear alternatives in the Standards—options—much like a decision box or if / then statements.

For example: If you use virtual, then take path B; if not, continue with path A's existing requirements. We believe such an approach would provide an easier transition

Likes 0

Dislikes 0

Response

Neil Swearingen - Salt River Project - 1,3,5,6 - WECC

Answer

Document Name

Comment

SRP has no additional comments.

Likes 0

Dislikes 0

Response

James Brown - California ISO - 2 - WECC

Answer

Document Name

Comment

The new CIP-005 standard provides more clarity around use of virtual infrastructure and virtual machines but will require 2-3 years for some companies to implement – this is not a like to like change. It is somewhat noteworthy that many entities have already implemented virtual infrastructure and are able to comply, even under audit scrutiny, to the current wording of the standards. As such, the CAISO believes current approved and implemented versions of the standards allow for virtualization. These changes would guide the adoption of virtualized environments, but any changes need to be backward compatible to support existing solutions.

General comment: Spell out acronyms in all requirement parts to ensure clear understanding.

Removable Media: Examples were removed. However, examples were still listed for Transient Cyber Asset. Examples are very helpful.

PAMS and PACS: Based on the implementations, mounted hardware or devices might not actually be mounted exactly at the Physical Security Perimeter. Consider rewording this.

Likes 0

Dislikes 0	

Response

Jennifer Wright - Sempra - San Diego Gas and Electric - 1,3,5

Answer	
Document Name	

Comment

SDG&E supports EEI’s comments submitted on our behalf.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,5,6 - SERC, Group Name Duke Energy

Answer	
Document Name	

Comment

Duke Energy does not have any additional comments at this time.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - MRO, Group Name Westar-KCPL

Answer	
Document Name	

Comment

Westar / Kansas City Power & Light support Edison Electric Institute’s (EEI) response to Question 13.

Likes 0	
Dislikes 0	

Response

Patricia Boody - Lakeland Electric - 1,3,5,6	
Answer	
Document Name	
Comment	
LAK realizes that the SDT is not yet developing an implementation plan. LAK recommends that the SDT consider these changes and the implications of major overhaul of existing CIP programs when developing the proposal for an implementation plan. LAK also recommends that NERC establish another group similar to the v5TAG for a pilot implementation of the revised standards.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI notes many improvements over the previous virtualization proposal, however the new, revised, and retired Glossary Terms; new and revised CIP-005 Requirements need to be further clarified. While the proposed changes achieve many of the desired goals (i.e., more broadly enabled virtualization), there remains some concerns that those changes may create unnecessary burden for registered entities that are not planning to deploy virtualization. For this reason, we ask the SDT to look for additional opportunities to better clarify how both solutions can be achieved to address the broad needs of the Industry.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2 - MRO,SERC,RF	
Answer	
Document Name	
Comment	
The proposed CIP-005-7 standard as currently written provides more clarity around use of virtual infrastructure and virtual machines and could require up to 3 years for some companies to implement. This does not equate to Backwards Compatibility as the standard does not allow entities to continue to operate "as is;" i.e. with no changes. In addition, a recent noteworthy observation is that multiple entities have implemented virtual infrastructure and have been found to be in compliance following an audit under the current version of the standards. As such, MISO recommends the SDT consider	

retaining the current approved and implemented versions of the standards "as is" and update the Technical Rationale and Justification document to describe how the standards support the implementation of virtualization with no change.

General comment: Spell out acronyms in all requirement parts to ensure clear understanding.

Removable Media: Examples were removed. However, examples were still listed for Transient Cyber Asset. Examples are very helpful.

PAMS and PACS: Based on the implementations, mounted hardware or devices might not actually be mounted exactly at the Physical Security Perimeter. Consider rewording this to allow for flexibility in location.

Likes 0

Dislikes 0

Response

Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5

Answer

Document Name

Comment

Please update the NERC Project Tracking Spreadsheet with a full list of standards that will be affected by these changes. In addition to what is listed, please add CIP-008, CIP-009, and CIP-011. In the future, consider adding CIP-013 due to the expectation of future versions including EACMS and firewalls.

There is an issue with this online comment form where it has not saved our Yes/No responses accurately and will not allow for manual changes. We have tried to provide context in each question to show whether Tri-State agrees with the modifications or not.

Likes 0

Dislikes 0

Response

Michael Johnson - Pacific Gas and Electric Company - 1,3,5 - WECC

Answer

Document Name

Comment

PG&E provides the following:

1 - PG&E submits the following concern regarding the proposed modification to the Physical Security Perimeter (PSP) definition:

Removal of the Cyber Asset types to be protected will lead to interpretation differences between Registered Entities and Audit Team on what should be physically protected. What is not indicated in the Technical Rationale document for the PSP modification is the method of indicating the Cyber Assets to be protected. PG&E assumes this will be done using appropriate modifications to the Applicable Systems column for each CIP-006 Requirement Part when those modifications are posted for comment.

If the above is not correct how Cyber Assets to be protected will be indicated, please indicate in later comment postings how those Cyber Assets will be indicated.

Likes 0

Dislikes 0

Response

Greg Davis - Georgia Transmission Corporation - 1

Answer

Document Name

Comment

GTC is concerned that the list of Applicable Systems identified in Section 4 of CIP-005 is not reflective of the “systems” listed within the requirements table. The requirements table and Section 4 of the standard should reflect/list the same potential “Applicable Systems” as applicable across and within the standard. Accordingly, GTC recommends that the SDT review this discrepancy and make the revisions necessary to ensure consistency.

Further, GTC is concerned that some of the “systems” listed as “Applicable Systems” within the requirements table are not necessarily systems and, therefore, do not necessarily easily lend themselves to identification of a particular asset or system. For this reason, such classification may result in each Responsible Entity attempting to “translate” such system into a set of associated assets, e.g., Electronic Security Perimeter and Electronic Security Zone. Such translation could vary greatly by and amongst Responsible Entities as well as the ERO and its auditors. GTC recommends that the SDT review these revisions to the “Applicable Systems” column to ensure that the objective and applicability is clear, unambiguous, and feasible.

GTC notes that the use of terms versus associated acronyms is inconsistent in the proposed draft of CIP-005, e.g., use of “IS” versus use of “Intermediate System.” GTC recommends the SDT evaluate the proposed draft for consistent usage of acronyms versus defined terms.

Finally, GTC notes that there was not an update to or an indication of review of VSLs or VRFs. It is recommended that such review occur to ensure that they remain consistent with the requirements of CIP-005.

Likes 0

Dislikes 0

Response

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the BES. Identification and categorization of BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-7:

4.2.3.1. Cyber systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Date: See “Project 2016-02 Virtualization Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** RAS that support the reliable operation of the Bulk Electric System; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BCS or SCI that hosts any portion of a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact BCS or SCI that hosts any portion of a low impact BCS is not required).

1.4. Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).

1.5. Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above or their associated EACMS, PACS or PCAs.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1. Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2. Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. **Compliance Monitoring Process:**

    1.1. **Compliance Enforcement Authority:** “Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

    1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

    The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

    - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
    - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
    - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

    1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, and	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			associated SCI, five percent or fewer of identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS and associated SCI, five or fewer identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium	For Responsible Entities with more than a total of 100 high and medium impact BCS and associated SCI, more than five percent but less than or equal to 10 percent of identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BCS and associated SCI, more than five but less than or equal to 10 identified BCS or associated SCI have not been categorized or have been	For Responsible Entities with more than a total of 100 high or medium impact BCS and associated SCI, more than 10 percent but less than or equal to 15 percent of identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BCS and associated SCI, more than 10 but less than or equal to 15 identified BCS or associated SCI have not been categorized or have been	associated SCI, more than 15 percent of identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS and associated SCI, more than 15 identified BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact BCS, and associated SCI, five percent or fewer high or medium BCS or associated SCI, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, or associated SCI, five or fewer high or medium BCS or associated SCI, have not been identified.	incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS and associated SCI, more than five percent but less than or equal to 10 percent high or medium BCS or associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS and associated SCI, more than five but less than or equal to 10 high or medium BCS or associated SCI have not been identified.	incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS and associated SCI, more than 10 percent but less than or equal to 15 percent high or medium BCS or associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS and associated SCI, more than 10 but less than or equal to 15 high or medium BCS or associated SCI have not been identified.	impact BCS and associated SCI, more than 15 percent of high or medium impact BCS or associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS and associated SCI, more than 15 high or medium impact BCS or associated SCI have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (Requirement R2 Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval.	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (Requirement R2 Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval.	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (Requirement R2 Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval.	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (Requirement R2 Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (Requirement R2 Part 2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Requirement R2 Part 2.2)	(Requirement R2 Part 2.2)	(Requirement R2 Part 2.2)	

D. Regional Variances

None.

E. Associated Documents

See “Project 2016-02 Virtualization Implementation Plan”.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
7	TBD	Virtualization conforming changes	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High Impact Rating**
   Each BCS used by and located at any of the following:
   - **1.1.** Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.
   - **1.2.** Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.
   - **1.3.** Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.
   - **1.4.** Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.
2. **Medium Impact Rating**
   Each BCS, not included in Section 1 above, associated with any of the following:
   - **2.1.** Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.
   - **2.2.** Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BCS that meet this criterion are those shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.
   - **2.3.** Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.
   - **2.4.** Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each RAS or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center, not included in the High Impact Rating, used to perform the reliability tasks of a Transmission Operator in real-time to monitor and control BES Transmission Lines with an "aggregate weighted value" exceeding 6000 according to the table below. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

Voltage Value of a Line	Weight Value per Line
less than 100 kV (not applicable)	(not applicable)
100 kV to 199 kV	250
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating

BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7~~6~~

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those ~~BES Cyber Systems~~BCS could have on the reliable operation of the BES. Identification and categorization of ~~BES Cyber Systems~~BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. **Balancing Authority**

4.1.2. **Distribution Provider that owns** one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~Remedial Action Scheme~~RAS where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-7~~6~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters~~logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

~~4.2.3.2.~~4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Date:** See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-002-6.~~

~~6. **Background:** This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**BES Cyber Systems**~~

~~The CIP Cyber Security Standards use the “BES Cyber System” term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware~~

~~protection to a grouping rather than individual Cyber Assets and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.~~

~~Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.~~

~~It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Reliable Operation of the BES~~

~~The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.~~

~~Real-time Operations~~

~~One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.~~

~~Categorization Criteria~~

~~The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement R1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact.~~

~~This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the CIP Cyber Security Standards.~~

~~Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems~~

~~BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:~~

- ~~**Electronic Access Control or Monitoring Systems (“EACMS”)** – Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.~~
- ~~**Physical Access Control Systems (“PACS”)** – Examples include: authentication servers, card systems, and badge control systems.~~
- ~~**Protected Cyber Assets (“PCA”)** – Examples include, to the extent they are within the ESP: file servers, FTP servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** ~~Remedial Action Schemes~~RAS that support the reliable operation of the Bulk Electric System; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact ~~BES Cyber System~~BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact ~~BES Cyber System~~BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact ~~BES Cyber System~~BCS or SCI that hosts any portion of a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact ~~BES Cyber Systems~~ BCS or SCI that hosts any portion of a low impact BCS is not required).

1.4. Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).

1.5. Identify associated SCI that hosts any portion of the medium impact ~~BES Cyber System~~BCS identified in Part 1.2 above or their associated EACMS, PACS or PCAs.

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1~~, and Parts 1.1, and 1.2, 1.4 and 1.5~~.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1. Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2. Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~**1.4. Additional Compliance Information:**~~

~~None.~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~6~~)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Systems~~BCS, and associated SCI, five percent or fewer of identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, five or fewer identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR	For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than five percent but less than or equal to 10 percent of identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and ~~BES Cyber Systems~~BCS and associated SCI, more than five but less than or equal to 10 identified ~~BES Cyber~~	For Responsible Entities with more than a total of 100 high or medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than 10 percent but less than or equal to 15 percent of identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and ~~BES Cyber Assets~~BCS and associated SCI, more than 10 but less than or equal to 15 identified ~~BES Cyber~~	~~Systems~~BCS and associated SCI, more than 15 percent of identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than 15 identified ~~BES Cyber Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, and associated SCI, five percent or fewer high or medium ~~BES Cyber Systems~~BCS or associated SCI, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, or associated SCI, five or fewer high or medium ~~BES Cyber Systems~~BCS or associated SCI, have not been identified.	~~Systems~~BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than five percent but less than or equal to 10 percent high or medium ~~BES Cyber Systems~~BCS or associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES~~	~~Assets~~ BCS or associated SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than 10 percent but less than or equal to 15 percent high or medium ~~BES Cyber Systems~~BCS or associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES~~	For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than 15 percent of high or medium impact ~~BES Cyber Systems~~BCS or associated SCI have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS and associated SCI, more than 15 high or medium impact ~~BES Cyber Systems~~BCS or associated SCI have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~Cyber Systems~~BCS and associated SCI, more than five but less than or equal to 10 high or medium ~~BES Cyber Systems~~BCS or associated SCI have not been identified.	~~Cyber Systems~~BCS and associated SCI, more than 10 but less than or equal to 15 high or medium ~~BES Cyber Systems~~BCS or associated SCI have not been identified.	
R2.	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (Requirement R2 Part ~~R~~2.1) OR The Responsible Entity did not complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (Requirement R2 Part ~~R~~2.1) OR The Responsible Entity failed to complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (Requirement R2 Part ~~R~~2.1) OR The Responsible Entity failed to complete its approval of the identifications required by	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (Requirement R2 Part ~~R~~2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (Requirement R2 Part ~~R~~2.2)	Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (Requirement R2 Part ~~R~~2.2)	Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (Requirement R2 Part ~~R~~2.2)	delegate according to Requirement R2 within 18 calendar months of the previous approval. (Requirement R2 Part ~~R~~2.2)

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan~~ for CIP-002-76~~.”
- ~~See Appendix 1. The Interpretation in Appendix 1 was developed under a prior version of the Reliability Standard, CIP-002-5.1, and is being carried forward to subsequent versions.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
7	TBD	Virtualization conforming changes	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High Impact Rating**
   Each ~~BES Cyber System~~BCS used by and located at any of the following:

   1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

   1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

   1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

   1.4. Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium Impact Rating**
   Each ~~BES Cyber System~~BCS, not included in Section 1 above, associated with any of the following:

   2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~ each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

   2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only ~~BES Cyber Systems~~BCS that meet this criterion are those shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

   2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each ~~Remedial Action Scheme (~~RAS~~)~~ or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center, not included in the High Impact Rating, used to perform the reliability tasks of a Transmission Operator in real-time to monitor and control BES Transmission Lines with an "aggregate weighted value" exceeding 6000 according to the table below. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center.

Voltage Value of a Line	Weight Value per Line
less than 100 kV (not applicable)	(not applicable)
100 kV to 199 kV	250
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating

~~BES Cyber Systems~~BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. ~~Remedial Action Schemes~~RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-6 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.~~

~~For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-6. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.~~

~~CIP-002-6~~

~~CIP-002-6 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, “…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES.”~~

~~The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-6. The concept includes a number of named BES reliability operating services. These named services include:~~

- ~~Dynamic Response to BES conditions~~

- ~~Balancing Load and Generation~~
- ~~Controlling Frequency (Real Power)~~
- ~~Controlling Voltage (Reactive Power)~~
- ~~Managing Constraints~~
- ~~Monitoring & Control~~
- ~~Restoration of BES~~
- ~~Situational Awareness~~
- ~~Inter-Entity Real-Time Coordination and Communication~~

~~Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.~~

~~Entity Registration~~	~~RC~~	~~BA~~	~~TOP~~	~~TO~~	~~DP~~	~~GOP~~	~~GO~~
~~Dynamic Response~~		~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Balancing Load & Generation~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Controlling Frequency~~		~~X~~				~~X~~	~~X~~
~~Controlling Voltage~~			~~X~~	~~X~~	~~X~~		~~X~~
~~Managing Constraints~~	~~X~~		~~X~~			~~X~~	
~~Monitoring and Control~~			~~X~~			~~X~~	
~~Restoration~~			~~X~~			~~X~~	
~~Situation Awareness~~	~~X~~	~~X~~	~~X~~			~~X~~	
~~Inter-Entity coordination~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~	~~X~~

~~Dynamic Response~~

~~The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:~~

- ~~Spinning reserves (contingency reserves)~~
    - ~~Providing actual reserve generation when called upon (GO,GOP)~~
    - ~~Monitoring that reserves are sufficient (BA)~~
- ~~Governor Response~~
    - ~~Control system used to actuate governor response (GO)~~
- ~~Protection Systems (transmission & generation)~~
    - ~~Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)~~
    - ~~Zone protection for breaker failure (DP, TO, TOP)~~
    - ~~Breaker protection (DP, TO, TOP)~~
    - ~~Current, frequency, speed, phase (TO,TOP, GO,GOP)~~
- ~~Remedial Action Schemes~~
    - ~~Sensors, relays, and breakers, possibly software (DP, TO, TOP)~~
- ~~Under and Over Frequency relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Under and Over Voltage relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Power System Stabilizers (GO)~~

~~Balancing Load and Generation~~

~~The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:~~

- ~~Calculation of Area Control Error (ACE)~~
    - ~~Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)~~
    - ~~Software used to perform calculation (BA)~~
- ~~Demand Response~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP,DP)~~
- ~~Manually Initiated Load shedding~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP, DP)~~
- ~~Non-spinning reserve (contingency reserve)~~

  - ~~Know generation status, capability, ramp rate, start time (GO, BA)~~
  - ~~Start units and provide energy (GOP)~~

~~Controlling Frequency (Real Power)~~

~~The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:~~

- ~~Generation Control (such as AGC)~~
  - ~~ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)~~
  - ~~Software to calculate unit adjustments (BA)~~
  - ~~Transmit adjustments to individual units (GOP)~~
  - ~~Unit controls implementing adjustments (GOP)~~
- ~~Regulation (regulating reserves)~~
  - ~~Frequency source, schedule (BA)~~
  - ~~Governor control system (GO)~~

~~Controlling Voltage (Reactive Power)~~

~~The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:~~

- ~~Automatic Voltage Regulation (AVR)~~
  - ~~Sensors, stator control system, feedback (GO)~~
- ~~Capacitive resources~~
  - ~~Status, control (manual or auto), feedback (TOP, TO,DP)~~
- ~~Inductive resources (transformer tap changer, or inductors)~~
  - ~~Status, control (manual or auto), feedback (TOP,TO,DP)~~
- ~~Static VAR Compensators (SVC)~~
  - ~~Status, computations, control (manual or auto), feedback (TOP, TO,DP)~~

~~Managing Constraints~~

~~Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:~~

- ~~Available Transfer Capability (ATC) (TOP)~~

- ~~Interchange schedules (TOP, RC)~~
- ~~Generation re-dispatch and unit commit (GOP)~~
- ~~Identify and monitor SOL's & IROL's (TOP, RC)~~
- ~~Identify and monitor Flow gates (TOP, RC)~~

~~Monitoring and Control~~

~~Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:~~

- ~~All methods of operating breakers and switches~~
  - ~~SCADA (TOP, GOP)~~
  - ~~Substation automation (TOP)~~

~~Restoration of BES~~

~~The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:~~

- ~~Restoration including planned cranking path~~
  - ~~Through black start units (TOP, GOP)~~
  - ~~Through tie lines (TOP, GOP)~~
- ~~Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)~~
- ~~Coordination (TOP, TO, BA, RC, DP, GO, GOP)~~

~~Situational Awareness~~

~~The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:~~

- ~~Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)~~
- ~~Change management (TOP,GOP,RC,BA)~~
- ~~Current Day and Next Day planning (TOP)~~
- ~~Contingency Analysis (RC)~~
- ~~Frequency monitoring (BA, RC)~~

~~Inter-Entity Coordination~~

~~The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and~~

~~operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:~~

- ~~Scheduled interchange (BA,TOP,GOP,RC)~~
- ~~Facility operational data and status (TO, TOP, GO, GOP, RC, BA)~~
- ~~Operational directives (TOP, RC, BA)~~

~~Applicability to Distribution Providers~~

~~It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.~~

~~Requirement R1:~~

~~Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.~~

~~Attachment 1~~

~~Overall Application~~

~~In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.~~

~~When the drafting team uses the term “Facilities,” there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as, “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-6, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may~~

~~be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.~~

~~In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.~~

~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.~~

~~High Impact Rating~~

~~This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.~~

~~The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.~~

~~Additional thresholds as specified in the criteria apply for this category.~~

~~Medium Impact Rating~~

~~No additional evaluation is necessary for BES Cyber Systems that have already been identified as high impact.~~

~~***Generation***~~

~~The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.~~

- ~~Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.~~

  ~~In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.~~

  ~~By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.~~

  ~~The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.~~

- ~~In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e. that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units~~

~~designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.~~

~~If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.~~

~~The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.~~

- ~~Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~

  ~~IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.~~

- ~~Criterion 2.9 categorizes BES Cyber Systems for Remedial Action Schemes as medium impact. Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.~~

- ~~Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.~~

- ~~Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~***Transmission***~~

~~*The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical*~~

~~*borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist.*~~

- ~~Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.~~

- ~~Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.~~

  ~~It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the “Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface.” This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.~~

- ~~Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:~~

  - ~~Excluded radial facilities that would only provide support for single generation facilities.~~
  - ~~Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.~~

  ~~The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.~~

~~Additionally, in Attachment 1 of NERC's "Integrated Risk Assessment Approach – Refinement to Severity Risk Index" document, the report used an average MVA line loading based on kV rating:~~

- ~~230 kV –> 700 MVA~~
- ~~345 kV –> 1,300 MVA~~
- ~~500 kV –> 2,000 MVA~~
- ~~765 kV –> 3,000 MVA~~

~~In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:~~

- ~~For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.~~
- ~~Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~
- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

~~Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.~~

1. ~~The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.~~

2. ~~The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4.: there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.~~

~~The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.~~

- ~~Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~
- ~~Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.~~
- ~~Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.~~
- ~~Criterion 2.9 designates as medium impact those BES Cyber Systems for those Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.~~
- ~~Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted~~

~~that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.~~

~~This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.~~

~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.~~

- ~~Criterion 2.12 categorizes medium impact BES Cyber Systems associated with Control Centers and backup Control Centers, including associated data centers, that monitor and control BES Transmission Lines with an aggregate weighted value of 6000 or higher, and that have not already been included in Part 1. The drafting team included additional qualifications in this criterion that would ensure the required level of impact to the BES is defined and a risk threshold associated to establish a floor for applicable medium impact BES Cyber Systems.~~

  ~~The total aggregated weighted value is used to account for the impact to the BES. The 6000 aggregate weighted value threshold defined in criterion 2.12 provides a sufficient differentiation for medium and low impact BES Cyber Systems associated with Control Centers that monitor and control BES Transmission Lines. SDT analysis of Transmission Control Centers validated that those facilities that may have significant impact are categorized at an appropriate level commensurate with the associated risk.~~

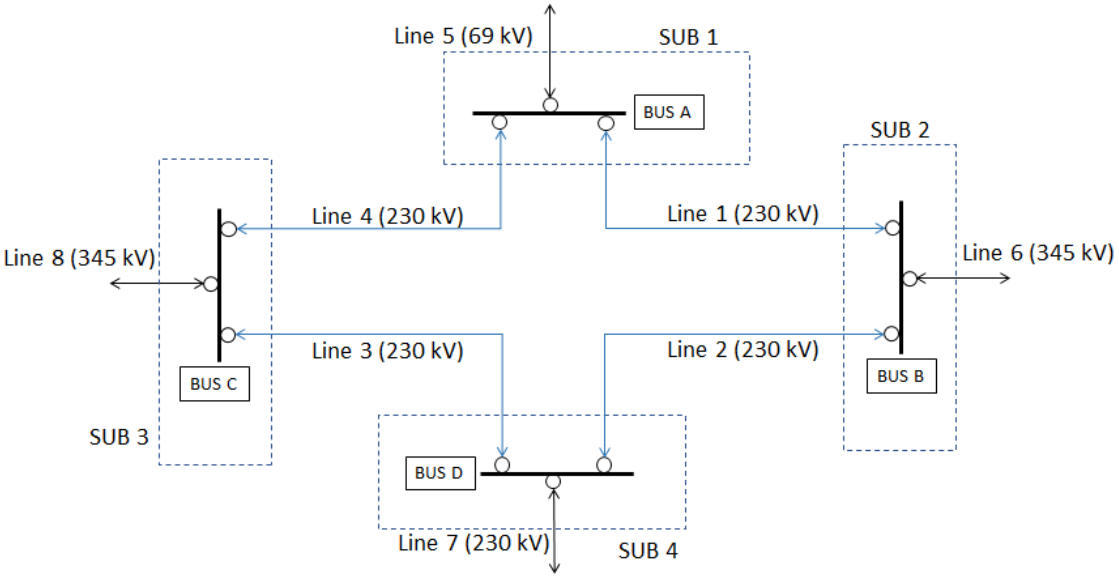
  ~~In the terms of applicable BES Transmission Lines, the following should be considered:~~

  - ~~All BES Transmission Lines that are energized at voltages between 100 kV and 499 kV and are monitored and controlled by a Control Center, including associated data center(s).~~

- ~~All BES Transmission Lines, including those that connect to neighboring entities, that are monitored and controlled by the Responsible Entity's Control Center, including associated data center(s).~~
- ~~Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line. For example, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~
- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. For example, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

~~Criterion 2.12 Examples:~~

~~In example 1 below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.~~



~~Example 1~~

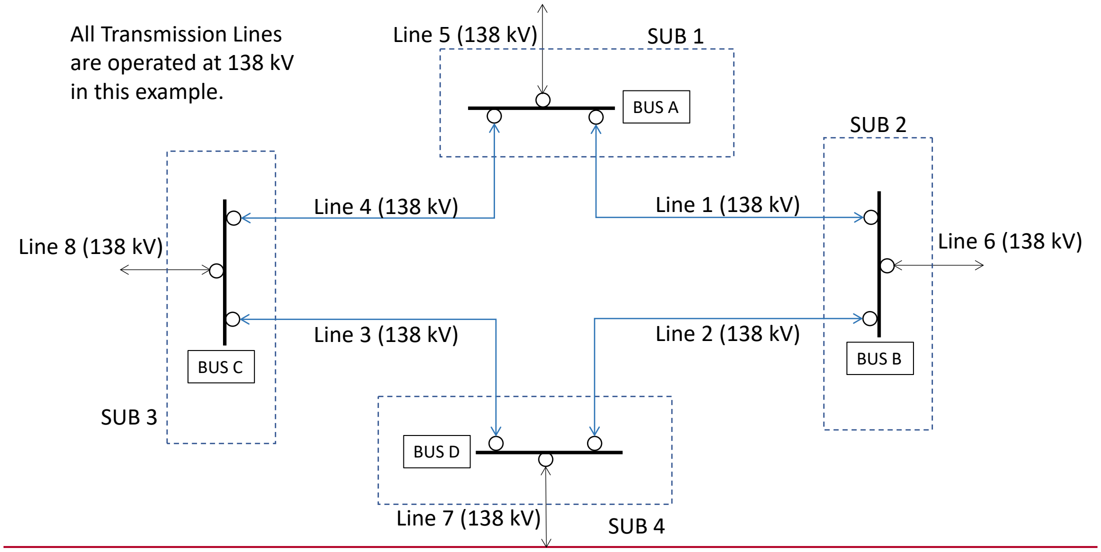
~~The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 6100, which is above the minimum threshold for the medium impact rating required in Criterion 2.12. In accordance with Criterion 2.12, the BES Cyber System(s) associated with the Control Center should be categorized as medium impact BES Cyber System(s).~~

~~Voltage Value of a Line~~	~~Weight Value per Line~~	~~Applicable Lines~~	~~Weighted Value~~
~~less than 100 kV~~ ~~(not applicable)~~	~~(not applicable)~~	~~Line 5~~	~~N/A~~
~~100 kV to 199 kV~~	~~250~~	~~None~~	~~0~~
~~200 kV to 299 kV~~	~~700~~	~~Line 1, Line 2, Line 3, Line 4, Line 7~~	~~3500~~
~~300 kV to 499 kV~~	~~1300~~	~~Line 6, Line 8~~	~~2600~~
~~500 kV and above~~	~~0~~	~~None~~	~~0~~

~~Calculation~~

~~700+700+700+700+700+1300+1300 = 6100~~

~~In the additional example below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.~~



~~Example 2~~

~~The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 2000, which is below the minimum threshold for a medium impact rating required in Criterion 2.12. The BES Cyber System(s) associated with the Control Center in this example should be categorized as a low impact BES Cyber System(s) pursuant to Criterion 3.1.~~

~~Voltage Value of a Line~~	~~Weight Value per Line~~	~~Applicable Lines~~	~~Weighted Value~~
~~less than 100 kV~~ ~~(not applicable)~~	~~(not applicable)~~	~~None~~	~~N/A~~
~~100 kV to 199 kV~~	~~250~~	~~Line 1, Line 2, Line 3, Line 4, Line 5, Line 6, Line 7, Line 8~~	~~2000~~
~~200 kV to 299 kV~~	~~700~~	~~None~~	~~0~~
~~300 kV to 499 kV~~	~~1300~~	~~None~~	~~0~~
~~500 kV and above~~	~~0~~	~~None~~	~~0~~

~~Calculation~~

~~250+250+250+250+250+250+250+250= 2000~~

- ~~Criterion 2.13 categorizes as Medium Impact those BA Control Centers that “control” 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Low Impact Rating~~

~~No additional evaluation is necessary for BES Cyber Systems that have already been identified as high or medium impact. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact. Note that low impact BES Cyber Systems do not require discrete identification, only identification of the asset containing the low impact BES Cyber System(s).~~

~~Restoration Facilities~~

- ~~Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.~~

  ~~In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.~~

  ~~The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.~~

  ~~Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.~~

  ~~BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~

  ~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection~~

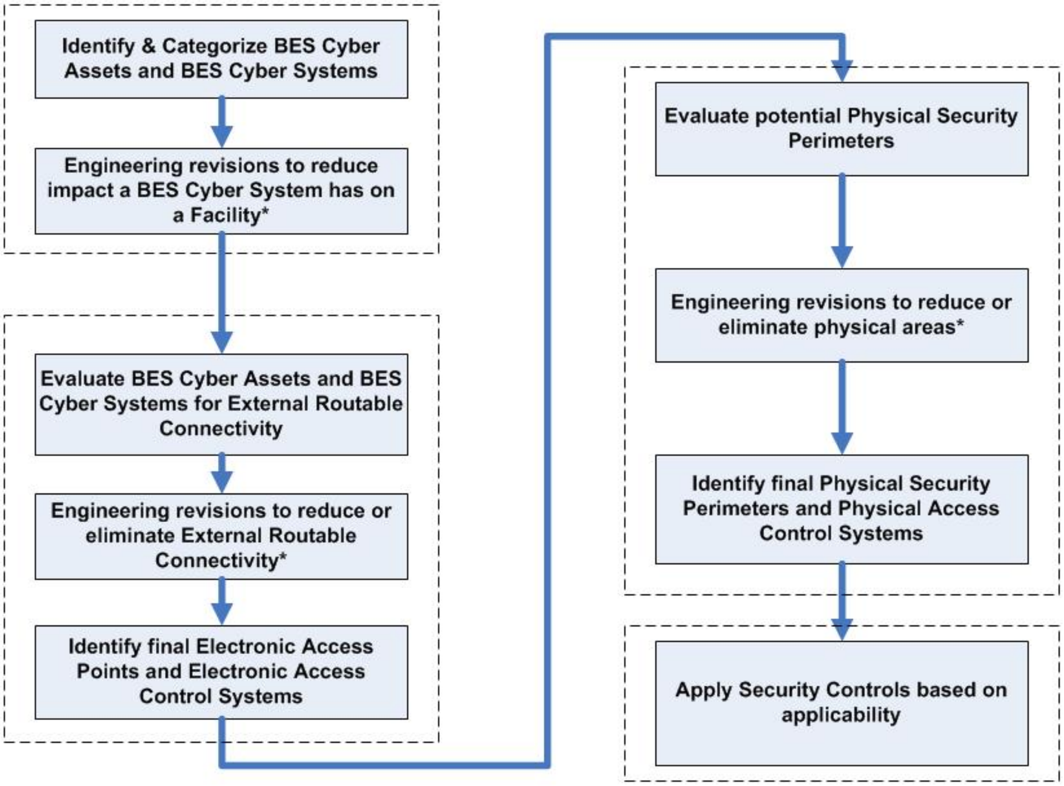
~~point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.~~

~~Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.~~

~~Use Case: CIP Process Flow~~

~~The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.~~

Overview (Generation Facility)



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

~~Rationale~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for R1:~~

~~BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~Rationale for R2:~~

~~The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.~~

~~Appendix 1~~

~~Requirement Number and Text of Requirement~~
~~CIP-002-5.1, Requirement R1~~ ~~R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:~~ ~~i. Control Centers and backup Control Centers;~~ ~~ii. Transmission stations and substations;~~ ~~iii. Generation resources;~~ ~~iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;~~ ~~v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and~~ ~~vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.~~ ~~1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;~~ ~~1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and~~

~~1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).~~

~~Attachment 1, Criterion 2.1~~

~~2. Medium Impact Rating (M)~~

~~Each BES Cyber System, not included in Section 1 above, associated with any of the following:~~

~~2.1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~

~~Questions~~

~~Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase “shared BES Cyber Systems.”~~

~~The Interpretation Drafting Team identified the following questions in the RFI:~~

1. ~~Whether the phrase “shared BES Cyber Systems” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~
2. ~~Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~
3. ~~If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~Responses~~

~~**Question 1: Whether the phrase “shared BES Cyber Systems,” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?**~~

~~The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states “Identify *each* of~~

~~the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)~~

~~Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:~~

> ~~The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~**Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?**~~

~~The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.~~

~~The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:~~

> ~~Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.~~

~~**Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?**~~

~~The phrase applies to each discrete BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-9

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. **Balancing Authority**

   4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. **Generator Operator**

   4.1.4. **Generator Owner**

   4.1.5. **Reliability Coordinator**

   4.1.6. **Transmission Operator**

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-9:

4.2.3.1. Cyber systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See "Project 2016-02 Virtualization Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS and associated SCI, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS and associated SCI, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS and their associated SCI that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their associated SCI is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS and associated SCI but did not address one of the nine topics required by Requirement R1. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS and associated SCI as required by	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS and associated SCI but did not address two of the nine topics required by Requirement R1. (Requirement R1 Part R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS and associated SCI as required by	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS and associated SCI but did not address three of the nine topics required by Requirement R1. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS and associated SCI as required by Requirement R1 within 17 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS and associated SCI but did not address four or more of the nine topics required by Requirement R1. (Requirement R1 Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS and associated SCI as required by Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	complete this review in less than or equal to 18 calendar months of the previous review. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR	(Requirement R1 Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS and associated SCI as

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (Requirement R1 Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI but did not address one of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its review	did complete this approval in less than or equal to 17 calendar months of the previous approval. (Requirement R1 Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI but did not address two of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not	The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI, but did not address three of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18	required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Requirement R1 Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI but did not address four or more of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002	complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Requirement R 1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for	calendar months of the previous review. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1 Part 1.2)	The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI as required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS and associated SCI as required by Requirement R1 by

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			containing low impact BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Requirement R1 Part 1.2)	its assets identified in CIP-002 containing low impact BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Requirement R1 Part 1.2)		the CIP Senior Manager within 18 calendar months of the previous approval. (Requirement R1 Part 1.2)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and associated SCI but failed to document cyber security awareness according	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and associated SCI but failed to reinforce cyber security practices at least	The Responsible Entity documented the physical access controls for its assets containing low impact BCS and associated SCI but failed to implement the physical security controls according to Requirement R2,	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BCS and associated SCI according to

<table>
<tr><th rowspan="2">R #</th><th rowspan="2">Time Horizon</th><th rowspan="2">VRF</th><th colspan="4">Violation Severity Levels (CIP-003-9)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td>to Requirement R2, Attachment 1, Section 1. (Requirement R2)
OR
The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2)
OR
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and associated SCI but failed to document</td><td>once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2)
OR
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and associated SCI but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2)
OR
The Responsible Entity documented its cyber security</td><td>Attachment 1, Section 2. (Requirement R2)
OR
The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BCS and associated SCI but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2)
OR
The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for assets containing low impact</td><td>Requirement R2, Attachment 1. (Requirement R2)</td></tr>
</table>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BCS and associated SCI but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1,	plan(s) for its assets containing low impact BCS and associated SCI but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BCS, per Cyber Asset capability according to Requirement R2, Attachment 1,	BCS and associated SCI but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to manage its TCA according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	Section 3.2 (Requirement R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BCS and associated SCI, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented	The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				its cyber security plan(s) for its assets containing low impact BCS and associated SCI but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable	Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Media, but failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to document mitigation for the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1,		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Section 5.2. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the change. (Requirement R3)	50 calendar days of the change. (Requirement R3)		not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Virtualization Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No.

Version	Date	Action	Change Tracking
			791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BCS.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding

Version	Date	Action	Change Tracking
			mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	TBD	Virtualization conforming changes	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS or their associated SCI

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, (2) the asset or the locations of the SCI hosting low impact BES Cyber Assets within the asset, and (3) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BCS or its associated SCI identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

  i. between a low impact BCS and a system(s) outside the asset containing low impact BCS;

  ii. between SCI hosting a low impact BCS and a system(s) outside the asset(s) containing the SCI hosting a low impact BCS;

  iii. using a routable protocol when entering or leaving the asset containing the low impact BCS or their associated SCI; and

  iv. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or their associated SCI, per Cyber Asset or VCA capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS or its associated SCI, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the TCA to a low impact BCS or its associated SCI (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or its associated SCI; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or its associated SCI.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BCS or their associated SCI

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS or their associated SCI within the asset; and
  b. The Cyber Asset(s), VCA, or SCI specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BCS, routable communication between a low impact BCS and systems outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BCS and systems outside the asset containing low impact BCS or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party

other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-9~~8~~

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-9~~8~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters (ESPs)~~logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

~~**4.2.3.2.**~~**4.2.3.3.** Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See “Project 2016-02 Virtualization Implementation Plan.” ~~for Project CIP-003-8~~

~~6. **Background:**~~

~~Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities’ management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.~~

~~The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.~~

~~The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term program may refer to the organization’s overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.~~

~~Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact ~~BES Cyber Systems~~BCS and associated SCI, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of ~~BES Cyber Systems~~BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for ~~BES Cyber Systems~~BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS and associated SCI, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS shall implement one or more documented cyber security plan(s) for its low impact ~~BES Cyber Systems~~BCS and their associated SCI that

include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact ~~BES Cyber Systems~~BCS or their associated SCI ~~BES Cyber Assets~~ is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~1.3. Compliance Monitoring and Assessment Processes:~~

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Investigations~~
- ~~Self-Reporting~~
- ~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None.~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact~~ BES Cyber Systems~~ BCS and associated SCI but did not address one of the nine topics required by Requirement R1. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS and associated SCI but did not address two of the nine topics required by Requirement R1. (Requirement R1 Part R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS and associated SCI but did not address three of the nine topics required by Requirement R1. (Requirement R1 Part ~~R~~1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS and associated SCI but did not address four or more of the nine topics required by Requirement R1. (Requirement R1 Part ~~R~~1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS and associated SCI as

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			and associated SCI as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS and associated SCI as required by Requirement R1 by the CIP Senior	and associated SCI as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Requirement R1 Part ~~R~~1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems BCS and associated SCI as required by Requirement R1 by the CIP Senior	R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Requirement R1 Part ~~R~~1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1)	required by Requirement R1. (Requirement R1 Part ~~R~~1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Requirement R1 ~~R~~Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI but did not address one of the six topics required by Requirement R1. (Requirement R1 ~~R~~Part 1.2)	Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Requirement R1 Part ~~R~~1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI but did not address two of the six topics required by Requirement R1. (Requirement R1 Part ~~R~~1.2)	OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI, but did not address three of the six topics required by Requirement R1. (Requirement R1 Part ~~R~~1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1 within 17 calendar	medium impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Requirement R1 Part ~~R~~1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI but did not address four or more of the six topics required by Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Requirement R1 ~~R~~Part 1.2) OR The Responsible Entity did not complete its	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Requirement R 1 Part ~~R~~1.2) OR The Responsible Entity did not complete its	months but did complete this review in less than or equal to 18 calendar months of the previous review. (Requirement R1 Part ~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval.	(Requirement R1 Part ~~R~~1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1. (Requirement R1 Part ~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Requirement R1 Part ~~R~~1.2)	approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Requirement R1 Part ~~R~~1.2)	(Requirement R1 Part ~~R~~1.2)	in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS and associated SCI as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Requirement R1 Part ~~R~~1.2)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low	The Responsible Entity documented its cyber security plan(s) for its assets containing low	The Responsible Entity documented the physical access controls for its assets containing low impact ~~BES Cyber~~	The Responsible Entity failed to document and implement one or more cyber security

<table>
<tr><th rowspan="2">R #</th><th rowspan="2">Time Horizon</th><th rowspan="2">VRF</th><th colspan="4">Violation Severity Levels (CIP-003-9~~8~~)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td>impact ~~BES Cyber Systems~~ BCS and associated SCI but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2)
OR
The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2)
OR
The Responsible Entity documented</td><td>impact ~~BES Cyber Systems~~ BCS and associated SCI but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2)
OR
The Responsible Entity documented its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI but failed to document physical security controls according to Requirement R2, Attachment 1,</td><td>~~Systems~~ BCS and associated SCI but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2)
OR
The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2)
OR</td><td>plan(s) for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI according to Requirement R2, Attachment 1. (Requirement R2)</td></tr>
</table>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI	Section 2. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all	The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to manage its TCA according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA, but failed to	Dial-up Connectivity that provides access to low impact ~~BES Cyber System(s)~~BCS, per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI, but failed to include the process for identification, classification, and response to Cyber Security Incidents	Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems~~ BCS and associated SCI but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to	the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~ BCS according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				document mitigation for the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified	The Responsible Entity has identified	The Responsible Entity has identified by name a	The Responsible Entity has not

R #	**Time Horizon**	**VRF**	**Violation Severity Levels (CIP-003-9~~8~~)**			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-9~~8~~)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			change in less than 40 calendar days of the change. (Requirement R4)	change in less than 50 calendar days of the change. (Requirement R4)	change. (Requirement R4)	OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ See "Project 2016-02 Virtualization Implementation Plan."

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact ~~BES Cyber Systems~~BCS.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	

Version	Date	Action	Change Tracking
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	TBD	Virtualization conforming changes	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact ~~BES Cyber Systems~~BCS or their associated SCI

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact ~~BES Cyber Systems~~BCS ratings can utilize policies, procedures, and processes for their high or medium impact ~~BES Cyber Systems~~BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact ~~BES Cyber Systems~~ BCS within the asset, (2) the asset or the locations of the SCI hosting low impact BES Cyber Assets within the asset, and (3~~2~~) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact ~~BES Cyber System(s)~~ BCS or its associated SCI identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. between a low impact ~~BES Cyber System(s)~~BCS and a ~~Cyber Asset(s)~~system(s) outside the asset containing low impact ~~BES Cyber System(s)~~BCS;

~~i.~~ii. between SCI hosting a low impact BCS and a system(s) outside the asset(s) containing the SCI hosting a low impact BCS;

~~ii.~~iii. using a routable protocol when entering or leaving the asset containing the low impact ~~BES Cyber System(s)~~BCS or their associated SCI; and

~~iii.~~iv. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact ~~BES Cyber System(s)~~ BCS or their associated SCI, per Cyber Asset or VCA capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. ~~Transient Cyber Asset~~ TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact ~~BES Cyber Systems~~ BCS or its associated SCI, through the use of ~~Transient Cyber Assets~~ TCA or Removable Media. The plan(s) shall include:

5.1 For ~~Transient Cyber Asset(s)~~ TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per ~~Transient Cyber Asset~~TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the ~~Transient Cyber Asset~~TCA to a low impact ~~BES Cyber System~~ BCS or its associated SCI (per ~~Transient Cyber Asset~~TCA capability):

- Review of antivirus update level;

- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset~~TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a ~~BES Cyber System~~ BCS or its associated SCI; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~ BCS or its associated SCI.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact ~~BES Cyber Systems~~BCS or their associated SCI

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact ~~BES Cyber Systems~~BCS or their associated SCI within the asset; and
  b. The Cyber Asset(s), VCA, or SCI specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact ~~BES Cyber Systems~~BCS, routable communication between a low impact ~~BES Cyber System(s)~~BCS and ~~a Cyber Asset(s)~~ systems outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact ~~BES Cyber System(s)~~BCS and ~~a Cyber Asset(s)~~systems outside the asset containing low impact ~~BES Cyber System(s)~~BCS or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the ~~BES Cyber System~~BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. ~~Transient Cyber Asset~~ TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~ TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.~~

~~If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.~~

~~Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.~~

~~Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC’s cyber security Reliability Standards will not be considered candidates for potential violations~~

~~although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.~~

~~For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:~~

~~1.1.1 Personnel and training (CIP-004)~~

~~Organization position on acceptable background investigations~~

~~Identification of possible disciplinary action for violating this policy~~

~~Account management~~

~~Electronic Security Perimeters (CIP-005) including Interactive Remote Access~~

~~Organization stance on use of wireless networks~~

~~Identification of acceptable authentication methods~~

~~Identification of trusted and untrusted resources~~

~~Monitoring and logging of ingress and egress at Electronic Access Points~~

~~Maintaining up-to-date anti-malware software before initiating Interactive Remote Access~~

~~Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access~~

~~Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access~~

~~For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls~~

~~Physical security of BES Cyber Systems (CIP-006)~~

~~Strategy for protecting Cyber Assets from unauthorized physical access~~

~~Acceptable physical access control methods~~

~~Monitoring and logging of physical ingress~~

~~System security management (CIP-007)~~

~~Strategies for system hardening~~

~~Acceptable methods of authentication and access control~~

~~Password policies including length, complexity, enforcement, prevention of brute force attempts~~

~~Monitoring and logging of BES Cyber Systems~~

~~Incident reporting and response planning (CIP-008)~~

~~Recognition of Cyber Security Incidents~~

~~Appropriate notifications upon discovery of an incident~~

~~Obligations to report Cyber Security Incidents~~

~~1.1.6 Recovery plans for BES Cyber Systems (CIP-009)~~

~~Availability of spare components~~

~~Availability of system backups~~

~~1.1.7 Configuration change management and vulnerability assessments (CIP-010)~~

~~Initiation of change requests~~

~~Approval of changes~~

~~Break-fix processes~~

~~1.1.8 Information protection (CIP-011)~~

~~Information access control methods~~

~~Notification of unauthorized information disclosure~~

~~Information access on a need-to-know basis~~

~~1.1.9 Declaring and responding to CIP Exceptional Circumstances~~

~~Processes to invoke special procedures in the event of a CIP Exceptional Circumstance~~

~~Processes to allow for exceptions to policy that do not violate CIP requirements~~

~~For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:~~

~~1.2.1 Cyber security awareness~~

~~Method(s) for delivery of security awareness~~

~~Identification of groups to receive cyber security awareness~~

~~1.2.2 Physical security controls~~

~~Acceptable approach(es) for selection of physical security control(s)~~

~~1.2.3 Electronic access controls~~

~~Acceptable approach(es) for selection of electronic access control(s)~~

~~1.2.4 Cyber Security Incident response~~

~~Recognition of Cyber Security Incidents~~

~~Appropriate notifications upon discovery of an incident~~

~~Obligations to report Cyber Security Incidents~~

~~1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~Acceptable use of Transient Cyber Asset(s) and Removable Media~~

~~Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media~~

~~Method(s) to request Transient Cyber Asset and Removable Media~~

~~1.2.6 Declaring and responding to CIP Exceptional Circumstances~~

~~Process(es) to declare a CIP Exceptional Circumstance~~

~~Process(es) to respond to a declared CIP Exceptional Circumstance~~

~~Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.~~

~~In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.~~

~~Requirement R2:~~

~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.~~

~~Requirement R2, Attachment 1~~

~~As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.~~

~~Guidance for each of the subject matter areas of Attachment 1 is provided below.~~

~~Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness~~

~~The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.~~

~~Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.~~

~~Requirement R2, Attachment 1, Section 2 – Physical Security Controls~~

~~The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.~~

~~The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with~~

~~locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.~~

~~The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.~~

~~Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.~~

~~User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.~~

~~Requirement R2, Attachment 1, Section 3 – Electronic Access Controls~~

~~Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.~~

~~When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).~~

~~When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.~~

~~In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.~~

~~The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.~~

~~Electronic Access Control Exclusion~~

~~In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.~~

~~Considerations for Determining Routable Protocol Communications~~

~~To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.~~

~~When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.~~

~~Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles~~

~~away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.~~

~~Determining Electronic Access Controls~~

~~Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.~~

~~Concept Diagrams~~

~~The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.~~

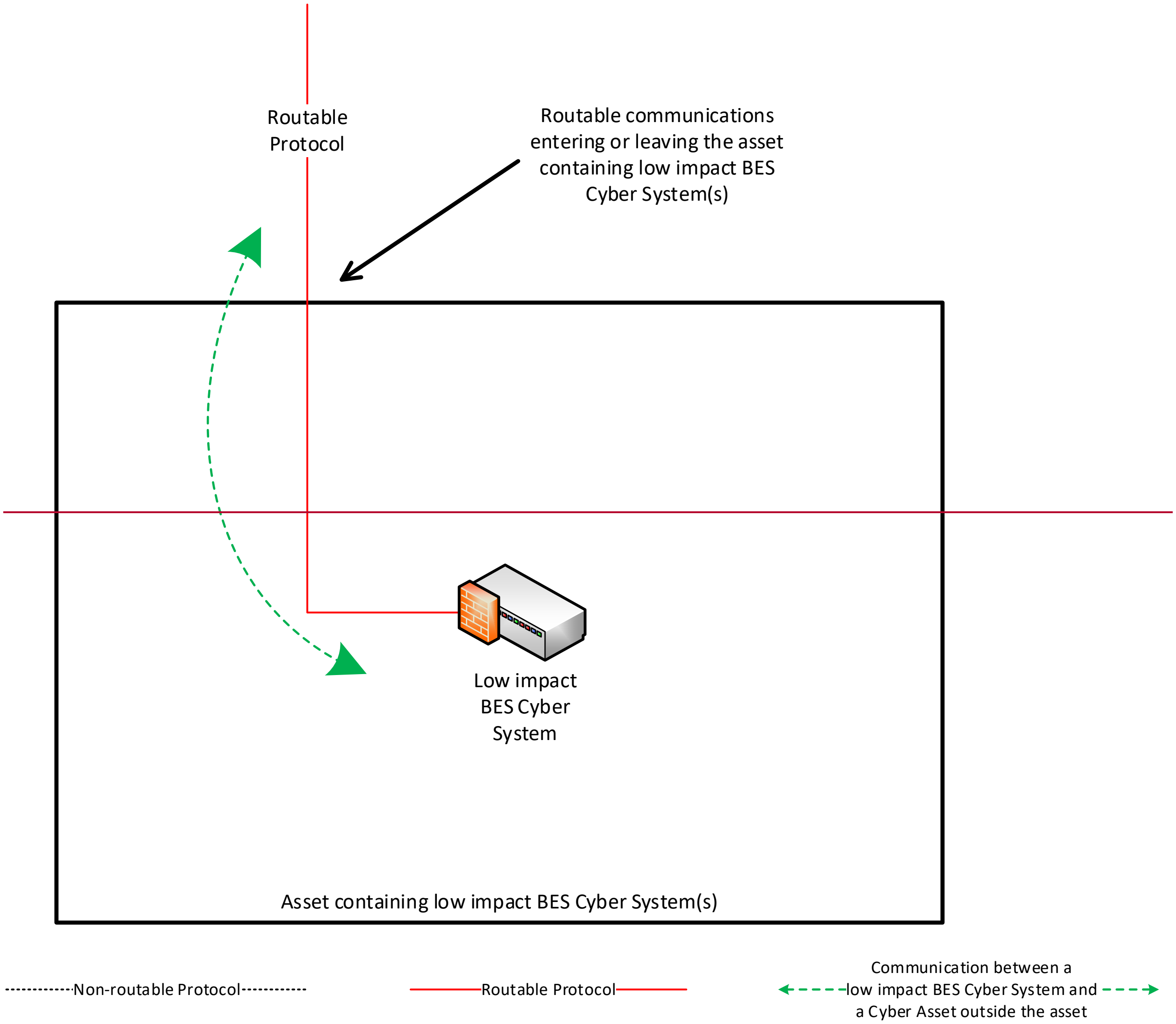
~~**NOTE:**~~

~~This is not an exhaustive list of applicable concepts.~~

~~The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.~~

~~Reference Model 1 – Host-based Inbound & Outbound Access Permissions~~

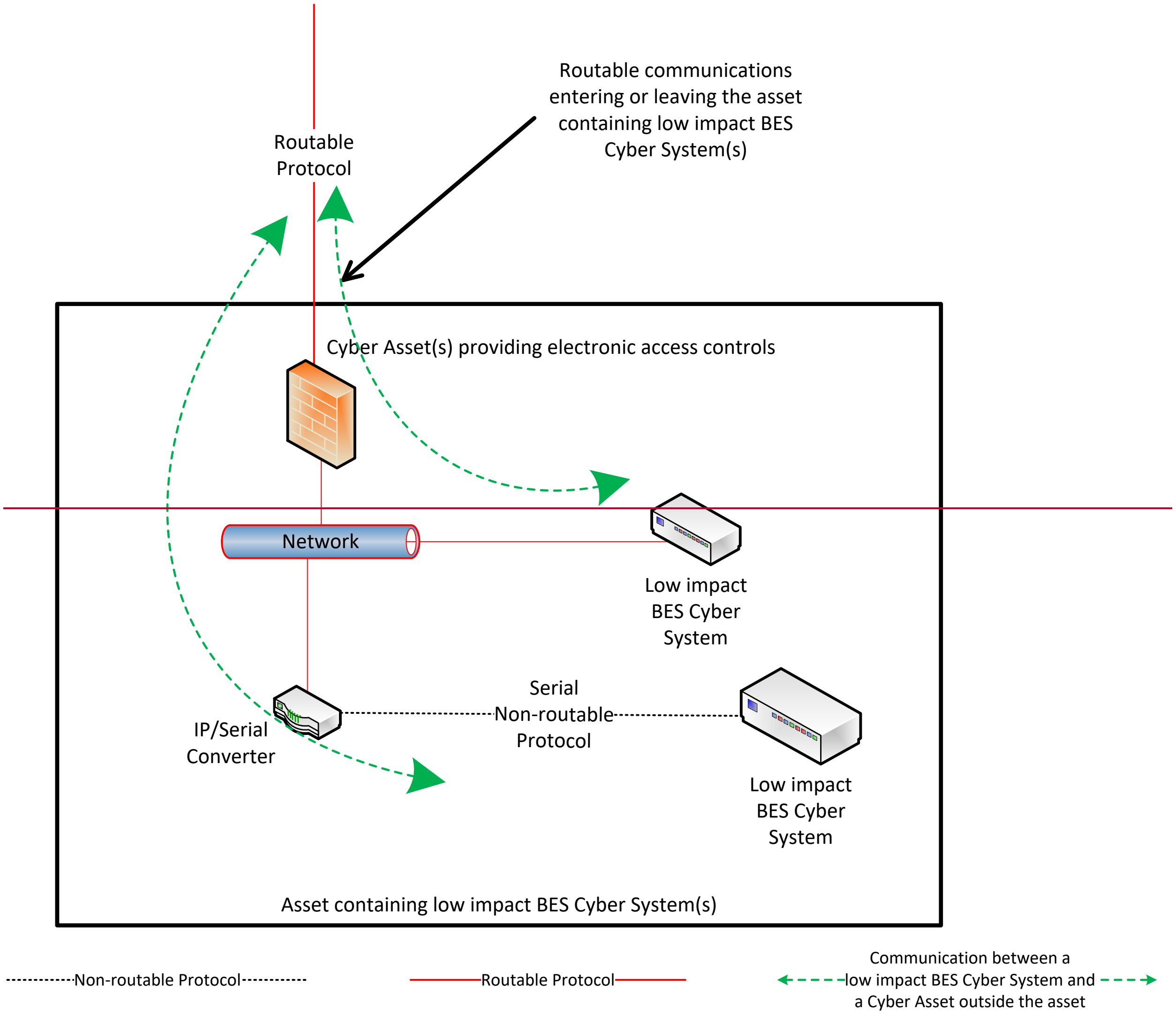
~~The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~Reference Model 1~~

~~Reference Model 2 – Network-based Inbound & Outbound Access Permissions~~

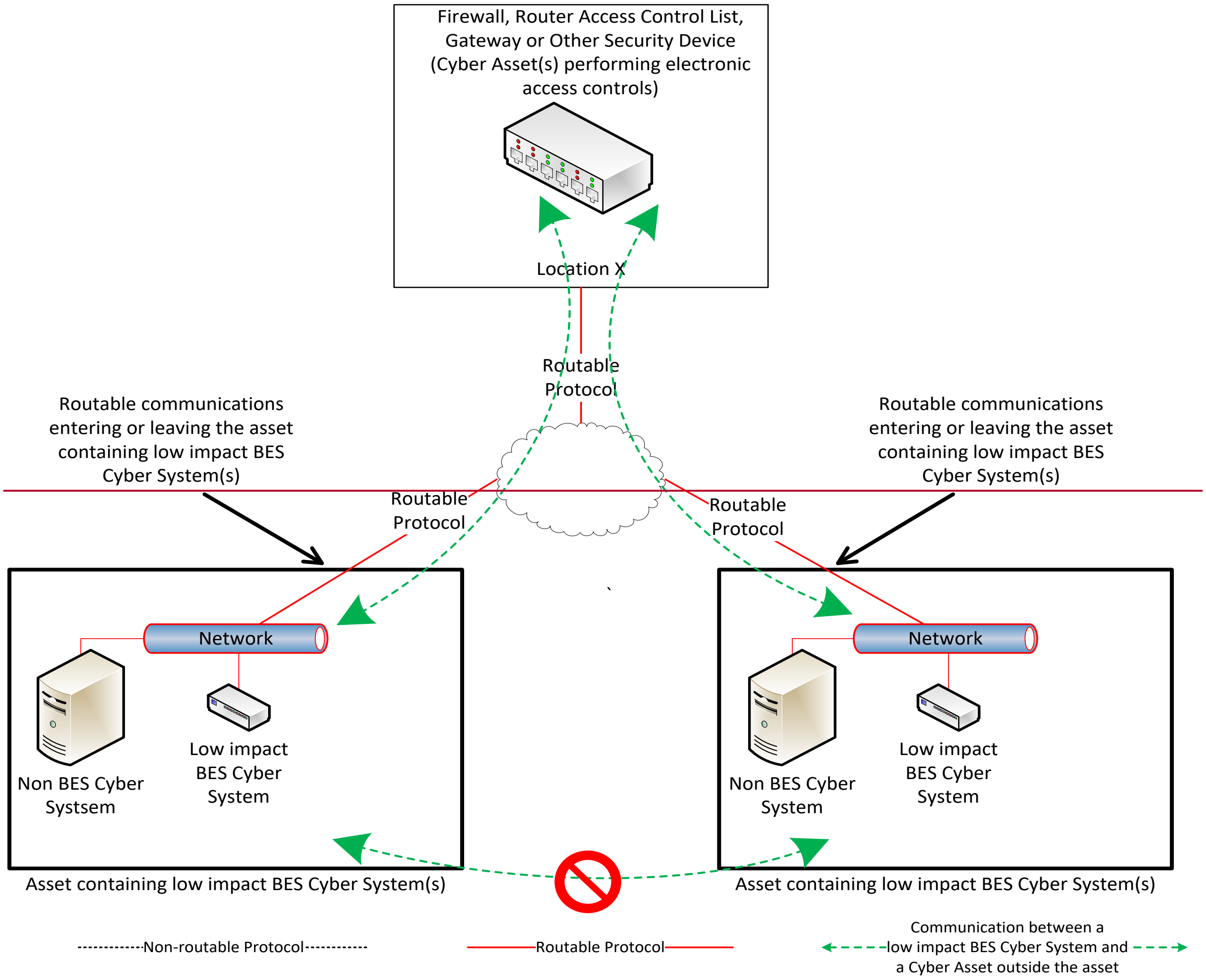
~~The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~Reference Model 2~~

~~Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions~~

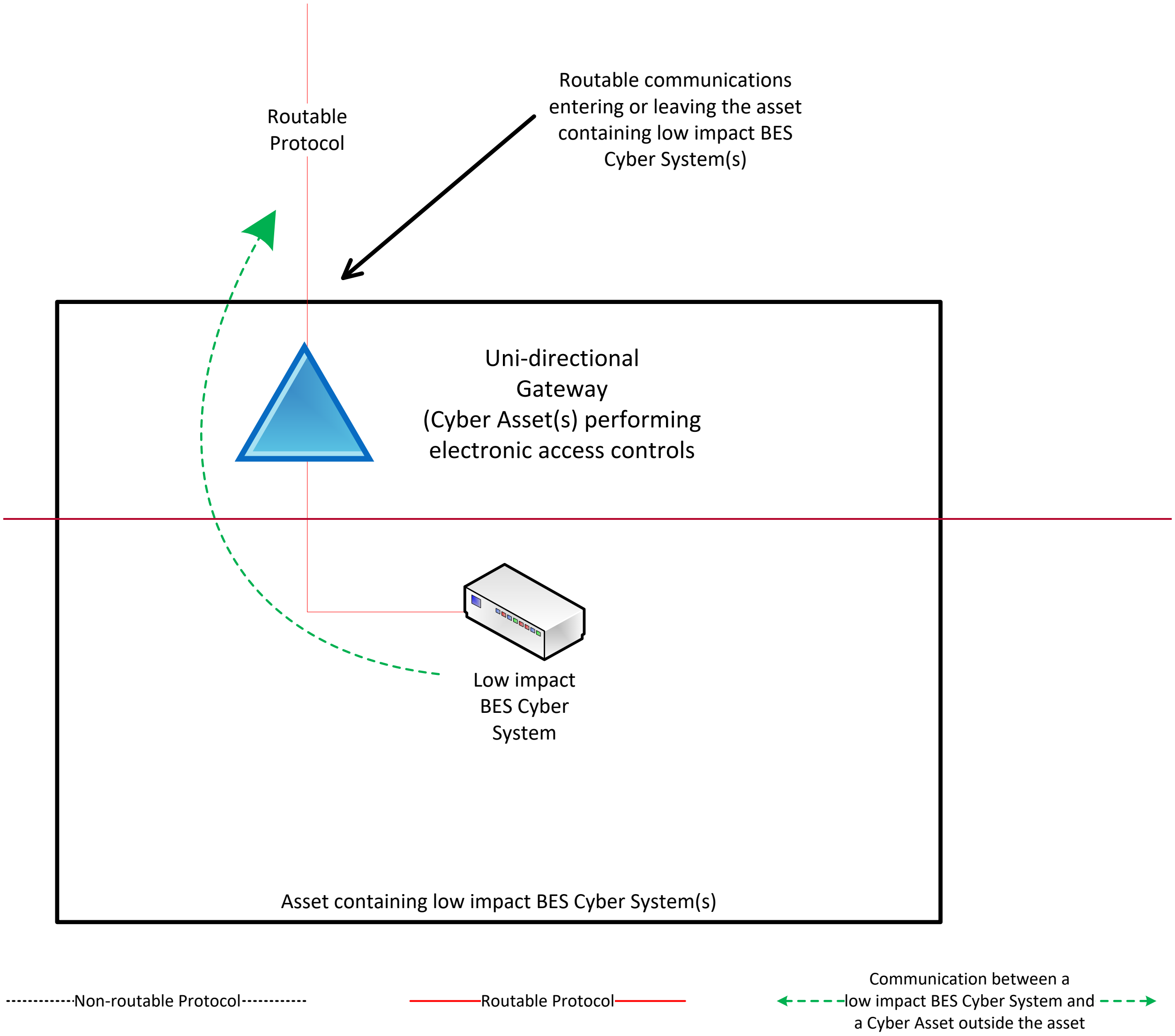
~~The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~Reference Model 3~~

~~Reference Model 4 – Uni-directional Gateway~~

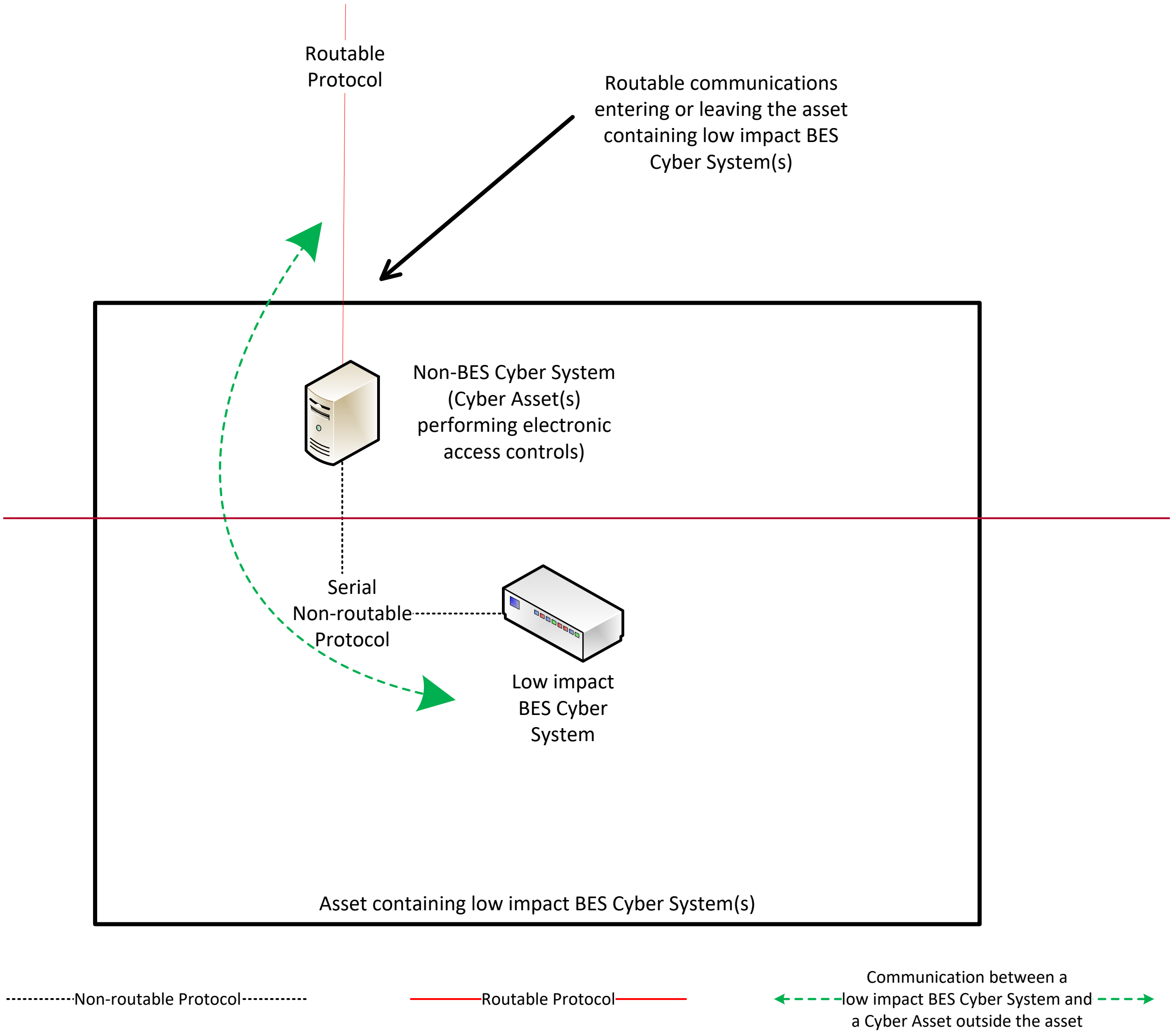
~~The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.~~



~~Reference Model 4~~

~~Reference Model 5 – User Authentication~~

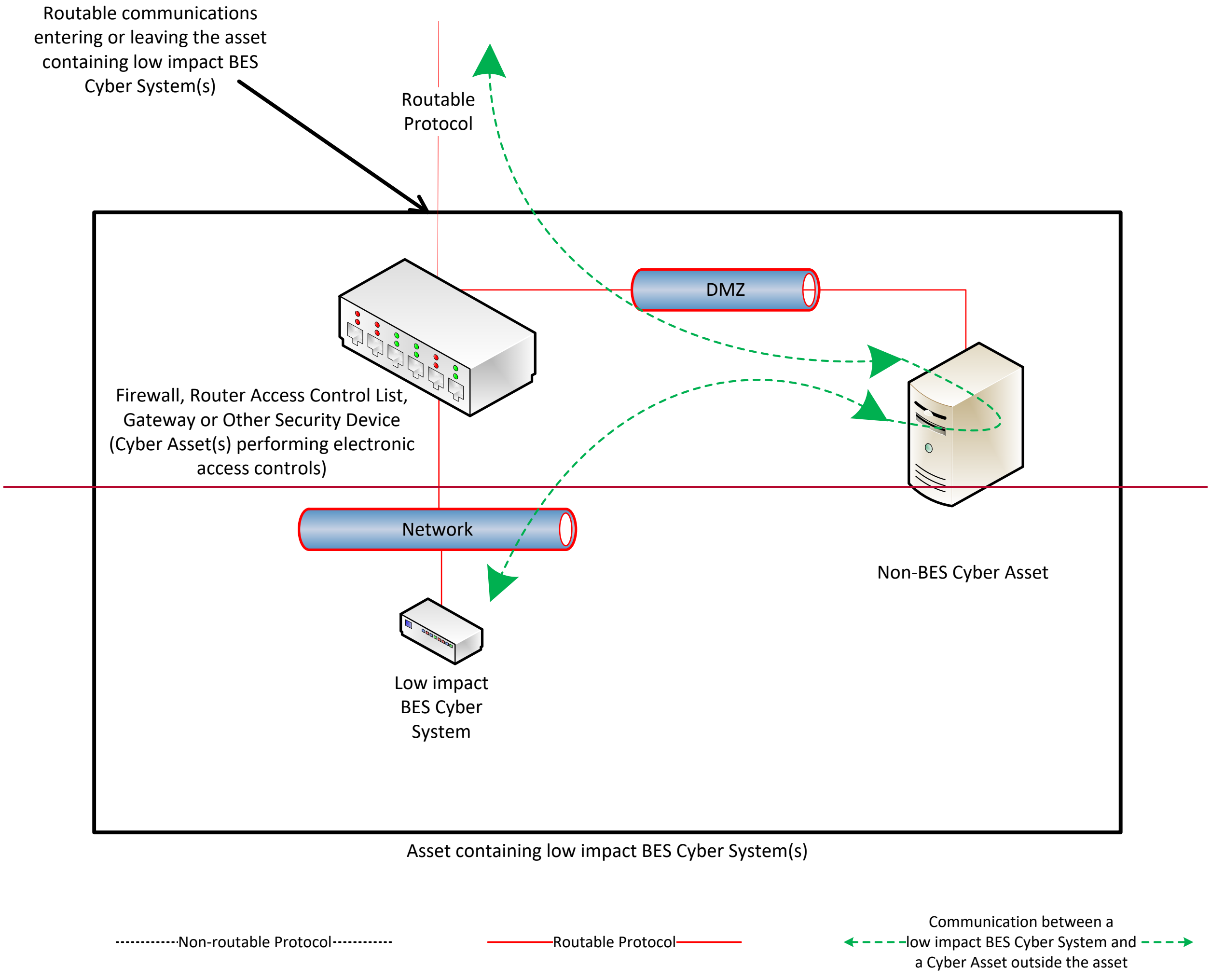
~~This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.~~



~~Reference Model 5~~

~~Reference Model 6 – Indirect Access~~

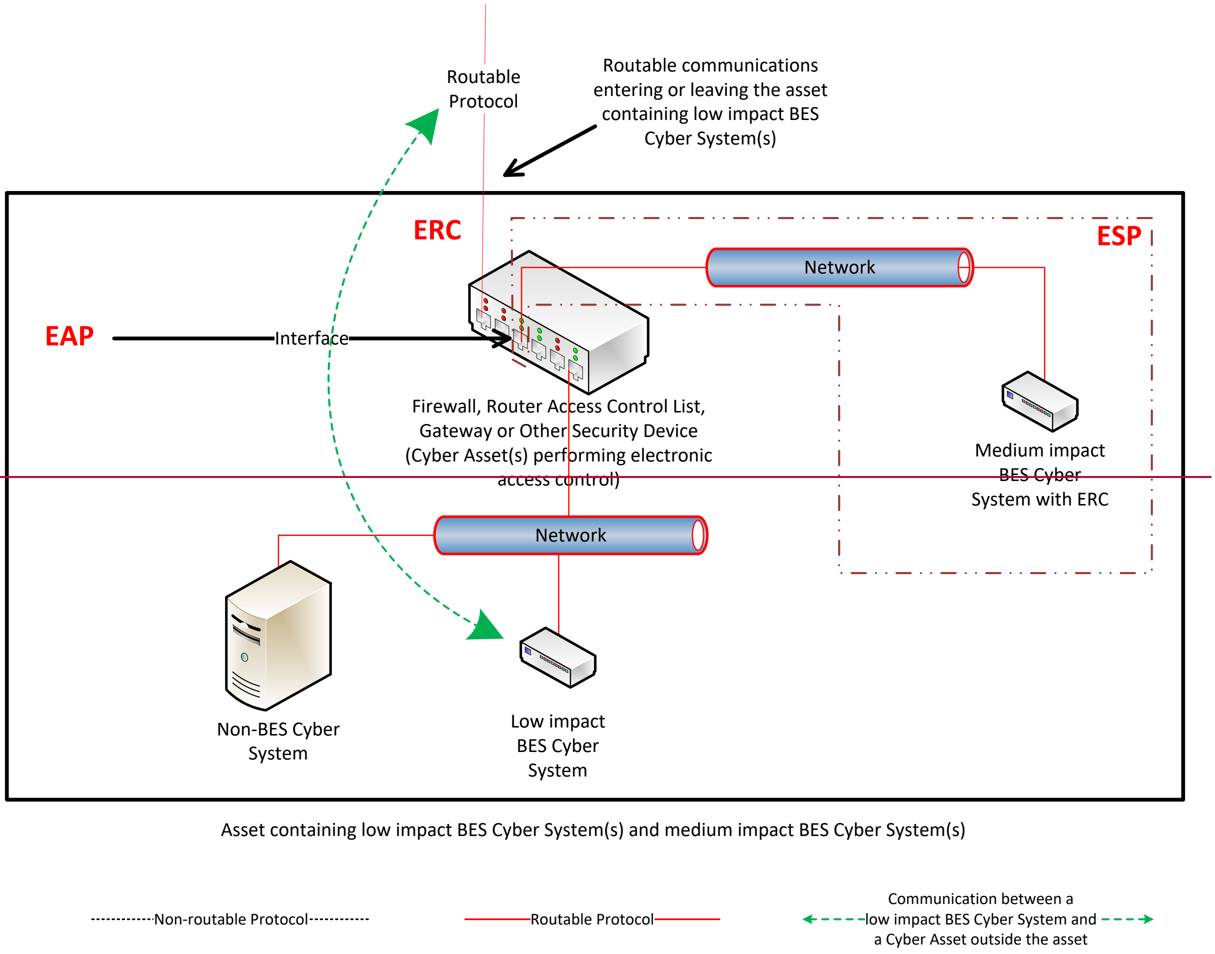
~~In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.~~



~~Reference Model 6~~

~~Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC~~

~~In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.~~



~~Reference Model 7~~

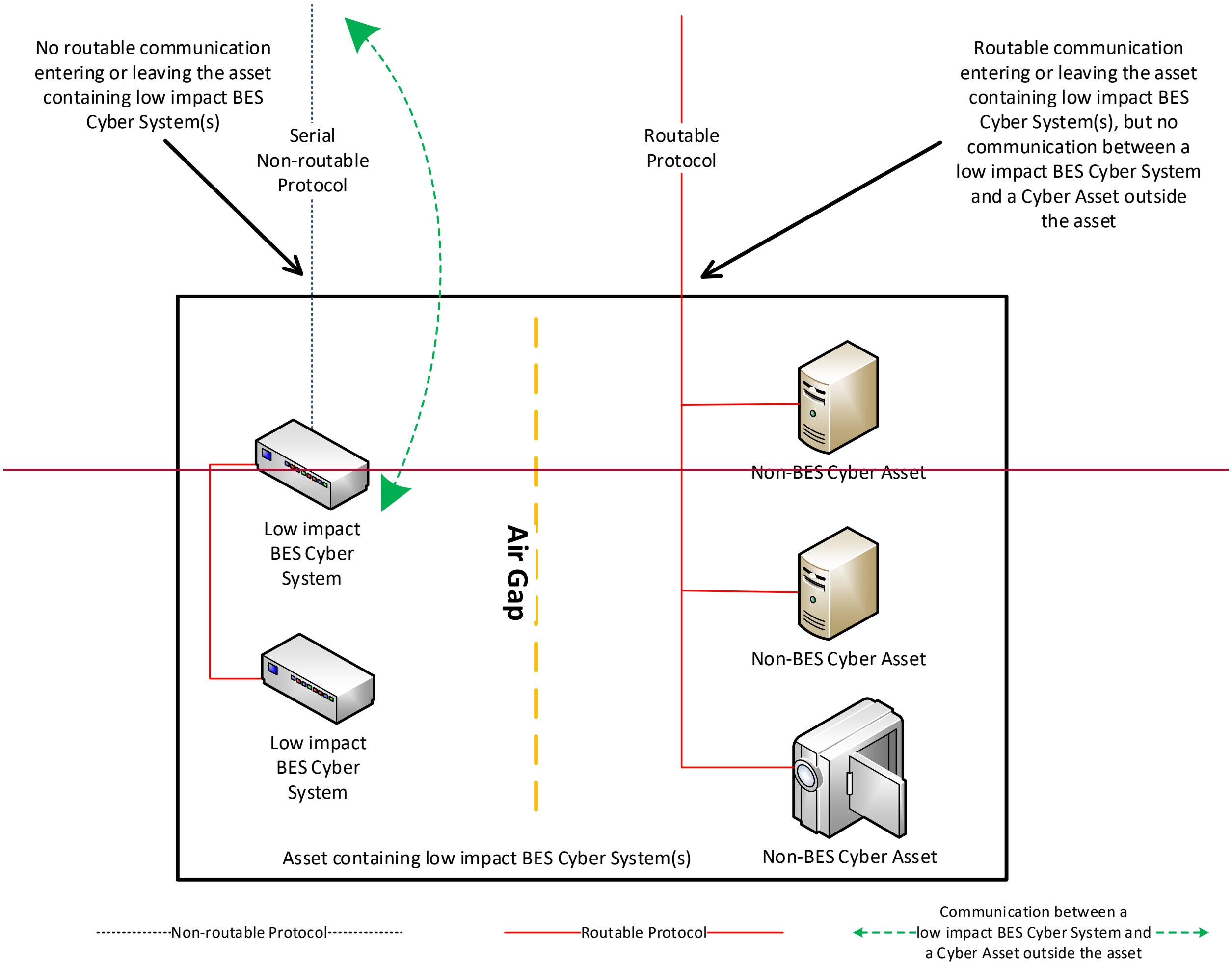
~~Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required~~

~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:~~

~~The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;~~

~~The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.~~

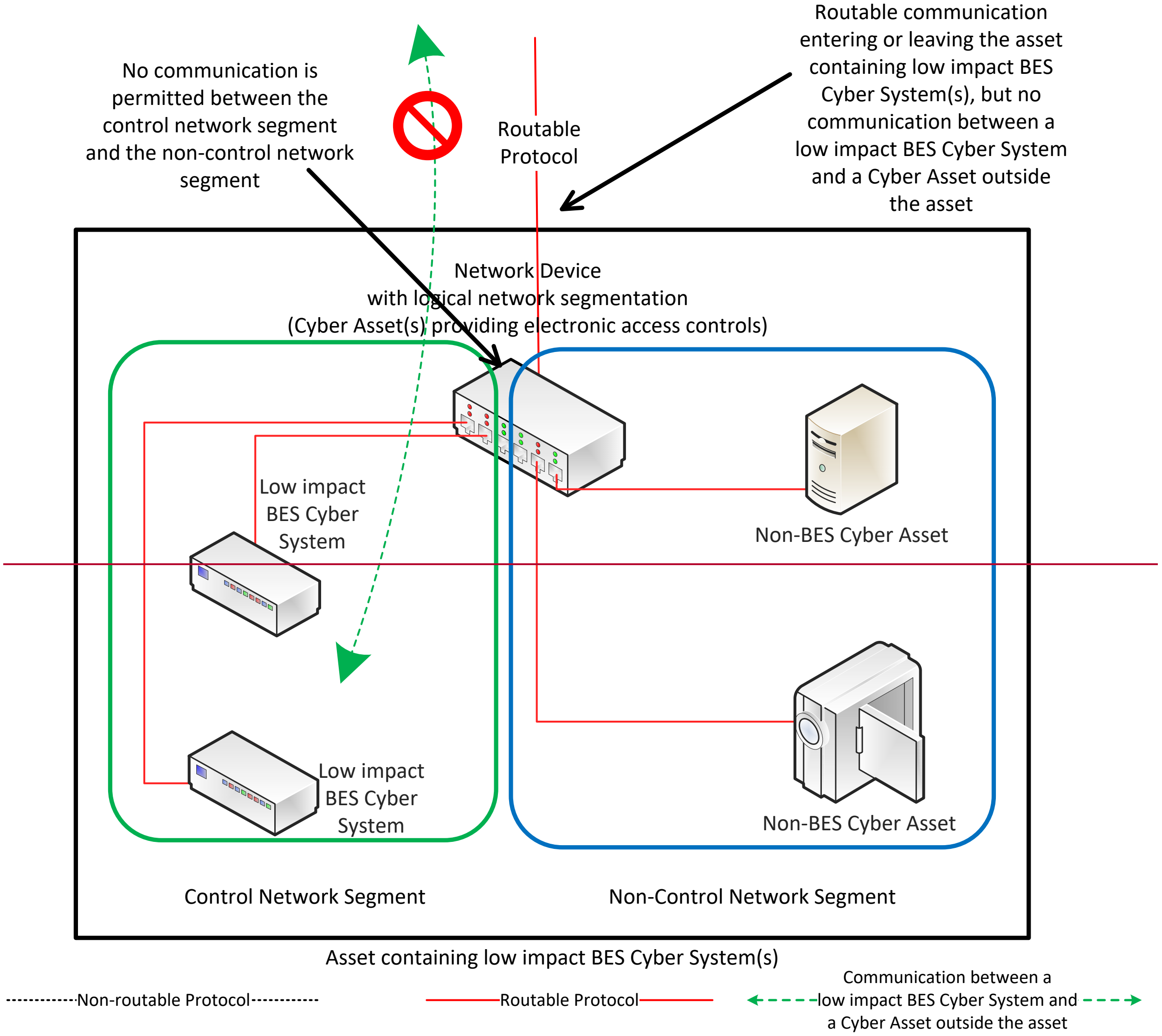
~~The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).~~



~~Reference Model 8~~

~~Reference Model 9 – Logical Isolation - No Electronic Access Controls Required~~

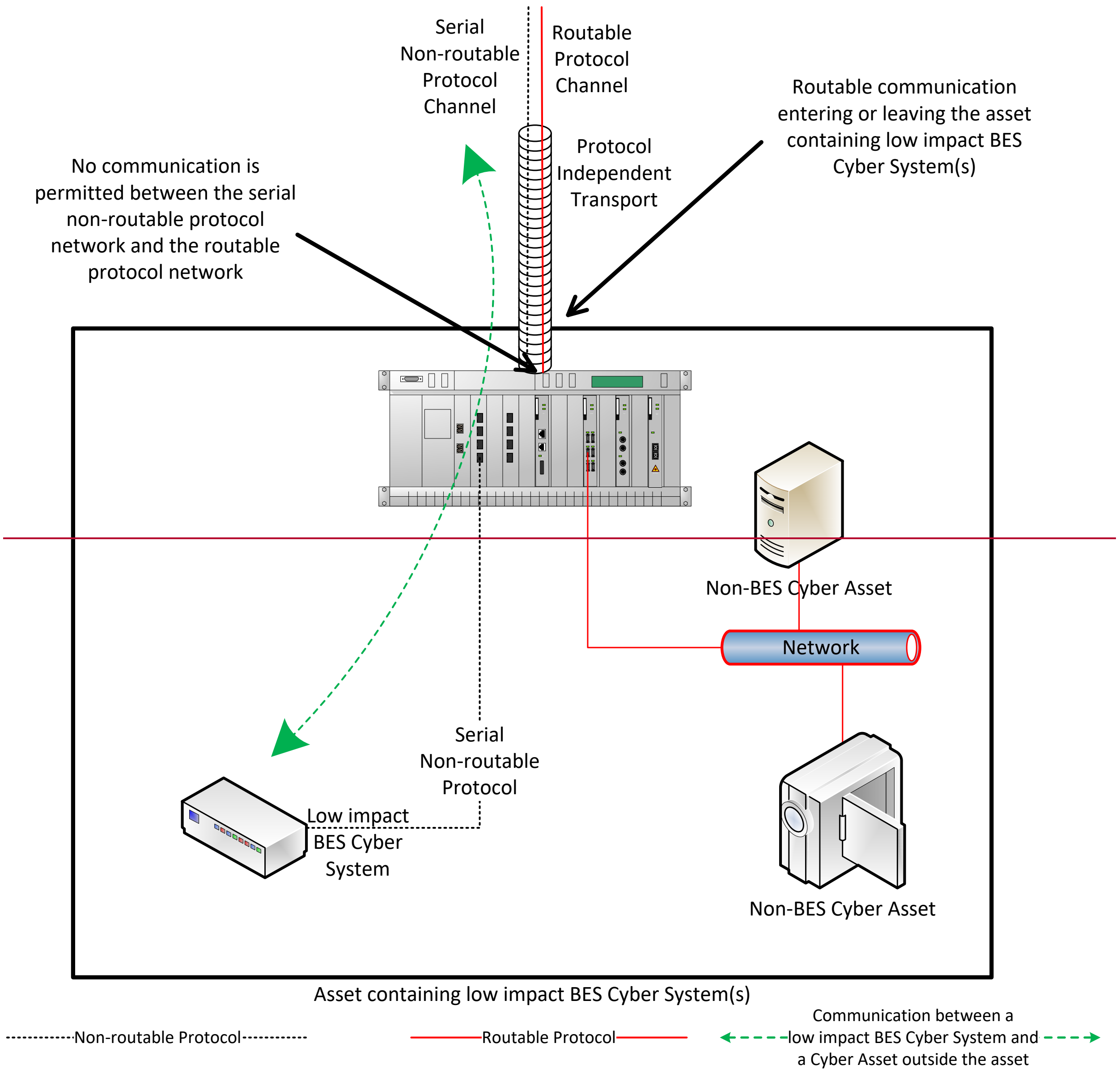
~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.~~



~~Reference Model 9~~

~~Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required~~

~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.~~



~~Reference Model 10~~

~~Dial-up Connectivity~~

~~Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.~~

~~Insufficient Access Controls~~

~~Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:~~

~~An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.~~

~~A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.~~

~~Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.~~

~~Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response~~

~~The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.~~

~~Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.~~

~~The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity’s response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.~~

~~For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, “A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.” The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.~~

~~Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.~~

~~Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets.~~

~~Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~Examples of these temporarily connected devices include, but are not limited to:~~

~~Diagnostic test equipment;~~

~~Equipment used for BES Cyber System maintenance; or~~

~~Equipment used for BES Cyber System configuration.~~

~~To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.~~

~~With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.~~

~~Malicious Code Risk Mitigation~~

~~The terms "mitigate", "mitigating", and "mitigation" are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.~~

~~Per Transient Cyber Asset Capability~~

~~As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.~~

~~Requirement R2, Attachment 1, Section 5.1 – Transient Cyber Asset(s) Managed by the Responsible Entity~~

~~For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.~~

~~**Section 5.1:**~~ ~~Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.~~

~~The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.~~

~~Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~The following is additional discussion of the methods to mitigate the introduction of malicious code.~~

~~Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.~~

~~Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.~~

~~When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.~~

~~If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~Requirement R2, Attachment 1, Section 5.2 – Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity~~

~~Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.~~

---

[1] ~~http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014~~

~~**Section 5.2.1:** Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.~~

~~Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.~~

~~Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.~~

~~Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.~~

~~Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.~~

~~Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.~~

~~**Section 5.2.2:** The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.~~

~~Requirement R2, Attachment 1, Section 5.3 – Removable Media~~

~~Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.~~

~~**Section 5.3:** Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.~~

~~As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in~~

~~conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.~~

~~**Requirement R3:**~~

~~The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.~~

~~**Requirement R4:**~~

~~As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.~~

~~The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.~~

~~Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.~~

~~Rationale for Requirement R2:~~

~~In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.~~

~~Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.~~

~~Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):~~

~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."~~

~~The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".~~

~~The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.~~

~~Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.~~

~~**Rationale for Section 5 of Attachment 1 (Requirement R2):**~~

~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "...provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~Rationale for Requirement R3:~~

~~The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.~~

~~FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for~~

~~responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.~~

~~Rationale for Requirement R4:~~

~~The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

~~In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for “clear lines of authority and ownership for security matters.” With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-7
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BCS.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:
All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-7:

4.2.3.1. Cyber systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. **Effective Dates:** See “Project 2016-02 Virtualization implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BCS and their associated SCI Medium Impact BCS and their associated SCI	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BCS or SCI.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. Electronic Access Control or Monitoring System (EACMS); and 2. Physical Access Control Systems (PACS) Medium Impact BCS, with External Routable Connectivity (ERC) or Interactive Remote Access (IRA), and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or - PACS SCI, with ERC or IRA, hosting Medium Impact BCS or their associated: - EACMS; or - PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS and SCI; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS and SCI's electronic interconnectivity and interoperability with other Cyber Assets and VCA, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, VCA or SCI, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BCS or their associated SCI that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven-years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven-year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven-year criminal history records check.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.4	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or - PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BCSI.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BCSI.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS: and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or - PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-7 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BCSI, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BCSI; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated EACMS or PACS. SCI with ERC or IRA hosting Medium Impact BCS or their associated EACMS or PACS.	A process to initiate removal of an individual's ability for unescorted physical access and IRA upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	For termination actions, revoke the individual's access to the designated storage locations for BCSI, whether physical or electronic (unless already revoked according to Requirement R5 Part 5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BCSI associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-7 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BCS and their associated: - EACMS SCI hosting High Impact BCS or their associated EACMS.	For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any applicable systems and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.5	High Impact BCS and their associated: - EACMS SCI hosting High Impact BCS or their associated EACMS.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: - Workflow or sign-off form showing password reset within 30 calendar days of the termination; - Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or - Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Requirement R1 Part 1.1)
R2	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security training program	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2 Part R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1)

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-004-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2)
OR
The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15</td><td>but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2)
OR
The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)</td><td>exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2)
OR
The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)</td><td>OR
The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2)
OR
The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)</td></tr>
</table>

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar months of the previous training completion date. (Requirement R2 Part 2.3)			
R3	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals.	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3)

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for	but did not confirm identity for two individuals. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized	(Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for	OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	one individual. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel	unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)	three individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)	electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)			
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories,	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BCSI is located. (Requirement R4 Part 4.1)

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify that access to the	verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BCSI storage locations, privileges were incorrect or	and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BCSI is correct and

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	designated storage locations for BCSI is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)	unnecessary. Requirement R4 Part (4.4)		necessary within 15 calendar months of the previous verification but for more than 15% of its BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)
R5	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BCSI, but for one individual, did not do so by the end of the next calendar day following the effective date and time of the	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (Requirement R5 Part 5.1) OR	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (Requirement R5 Part 5.1) OR	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BCSI storage locations. (Requirement R5 Part R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action but

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	termination action. (Requirement R5 Part 5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (Requirement R5 Part 5.4) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BCSI but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BCSI but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (Requirement R5 Part 5.3)	did not initiate those removals for three or more individuals. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2)

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more	termination action. (Requirement R5 Part 5.3)		

R #	Violation Severity Levels (CIP-004-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Requirement R5 Part 5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Virtualization Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata

Version	Date	Action	Change Tracking
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BCS.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-7 ~~6~~

3. Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting ~~BES Cyber Systems~~BCS.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

~~4.1.6.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-7~~6~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters~~logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

~~4.2.3.2.~~4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Dates: See "Project 2016-02 Virtualization implementation Plan." ~~for CIP-004-6~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7~~6~~ Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact ~~BES Cyber Systems~~ BCS and their associated SCI Medium Impact ~~BES Cyber Systems~~ BCS and their associated SCI	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to ~~BES Cyber Systems~~BCS or SCI.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-7~~6~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. Electronic Access Control or Monitoring System (EACMS); and 2. Physical Access Control Systems (PACS) Medium Impact ~~BES Cyber Systems~~BCS, with External Routable Connectivity (ERC) or Interactive Remote Access (IRA), and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI, with ERC or IRA, hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for ~~BES Cyber Systems~~ BCS and SCI; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a ~~BES Cyber System's~~ BCS and SCI's electronic interconnectivity and interoperability with other Cyber Assets and VCA, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, VCA or SCI, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

CIP-004-7~~6~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to ~~BES Cyber Systems~~ BCS or their associated SCI that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or - PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven-~~-~~years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven-~~-~~year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven-~~-~~year criminal history records check.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or - PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~ IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or - PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-7~~6~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.5	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC- or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or - PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA ~~-~~and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for ~~BES Cyber System Information~~BCSI.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for ~~BES Cyber System Information~~BCSI.

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or IRA and their associated: 1. EACMS: and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or - PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: - Dated -documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or - Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA -and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or - PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

CIP-004-7~~6~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA -and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or - PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	Verify at least once every 15 calendar months that access to the designated storage locations for ~~BES Cyber System Information~~BCSI, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for ~~BES Cyber System Iinformation~~BCSI; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-7~~6~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-7~~6~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated EACMS or PACS. SCI with ERC or IRA hosting Medium Impact BCS or their associated EACMS or PACS.	A process to initiate removal of an individual's ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-7~~6~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: - EACMS; or PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: - EACMS; or - PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-7~~6~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC or ~~Interactive Remote Access~~IRA and their associated: 1. EACMS; and 2. PACS SCI hosting High Impact BCS or their associated: • EACMS; or • PACS SCI with ERC or IRA hosting Medium Impact BCS or their associated: • EACMS; or • PACS	For termination actions, revoke the individual's access to the designated storage locations for ~~BES Cyber System Information~~BCSI, whether physical or electronic (unless already revoked according to Requirement R5 Part 5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing ~~BES Cyber System Information~~BCSI associated with the terminations and dated within the next calendar day of the termination action.

CIP-004-7~~6~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.4	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High Impact BCS or their associated EACMS.	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any ~~individual~~ applicable ~~BES Cyber Assets~~systems and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.5	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High Impact BCS or their associated EACMS.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~1.3. Compliance Monitoring and Assessment Processes:~~

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Requirement R1 Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Requirement R1 Part 1.1)
R2	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1)	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2 Part R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)	training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)	Requirement Parts 2.1.1 through 2.1.9. (Requirement R2 Part 2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Requirement R2 Part 2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	access within 15 calendar months of the previous training completion date. (Requirement R2 Part 2.3)			
R3	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals.	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in	unescorted physical access but did not confirm identity for two individuals. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized	(Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for	or more individuals. (Requirement R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (Requirement R3 Part 3.1 & Part 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	3.2.1 and 3.2.2 for one individual. (Requirement R3 Part 3.2 & Part 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not	electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)	three individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (Requirement R3 Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (Requirement R3 Part 3.5)			
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where ~~BES Cyber System~~

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its ~~BES Cyber~~applicable ~~S~~systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its ~~BES Cyber S~~applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System Information~~BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than	groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its ~~BES Cyber S~~applicable systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System Information~~BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its ~~BES Cyber System Information~~BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)	~~Information~~BCSI is located. (Requirement R4 Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Requirement R4 Part 4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its ~~BES Cyber~~applicable ~~S~~systems, privileges were incorrect or unnecessary. (Requirement R4 Part 4.3) OR

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	that access to the designated storage locations for ~~BES Cyber System Information~~BCSI is correct and necessary within 15 calendar months of the previous verification but for 5% or less of its ~~BES Cyber System Information~~BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)	(or equal to) 10% of its ~~BES Cyber System Information~~BCSI storage locations, privileges were incorrect or unnecessary. Requirement R4 Part (4.4)		The Responsible Entity has implemented processes to verify that access to the designated storage locations for ~~BES Cyber System Information~~BCSI is correct and necessary within 15 calendar months of the previous verification but for more than 15% of its ~~BES Cyber System Information~~BCSI storage locations, privileges were incorrect or unnecessary. (Requirement R4 Part 4.4)
R5	The Responsible Entity has implemented one or more process(es) to revoke the individual’s access to the designated storage locations for ~~BES Cyber System~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action but did not	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or ~~BES Cyber System Information~~BCSI storage locations. (Requirement R5 Part R5) OR

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	~~Information~~BCSI, but for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action. (Requirement R5 Part 5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (Requirement R5 Part 5.4)	24 hours of the termination action but did not initiate those removals for one individual. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more	initiate those removals for two individuals. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for ~~BES Cyber System~~	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Requirement R5 Part 5.2)

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more process(es) to determine and document	process(es) to revoke the individual's access to the designated storage locations for ~~BES Cyber System Information~~BCSI but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (Requirement R5 Part 5.3)	~~Information~~BCSI but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action. (Requirement R5 Part 5.3)	

R #	Violation Severity Levels (CIP-004-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Requirement R5 Part 5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~See "Project 2016-02 Virtualization Implementation Plan."

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact ~~BES Cyber Systems~~BCS.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Logical Isolation

2. **Number:** CIP-005-8

3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to and from the system and logically isolating all other communication to reduce the likelihood of misoperations or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Date: See Project 2016-02 Virtualization Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Logical Isolation*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Logical Isolation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Logical Isolation

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BCS connected to a network via a routable protocol and their associated: 1. Protected Cyber Asset (PCA); 2. Physical Access Control Systems (PACS) hosted on SCI; and 3. Electronic Access Control or Monitoring System (EACMS) hosted on SCI Medium Impact BCS connected to a network via a routable protocol and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI	Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems such as: • Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • SCI configuration or policies (hypervisor, fabric, backplane, or SAN configuration); that enforces electronic access control and logical isolation and documents the business need.

CIP-005-8 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	SCI hosting High or Medium Impact BCS or their associated: - PCA; - PACS; or - EACMS Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PCA; - PACS; or - EACMS EACMS that perform logical isolation for a High Impact BCS EACMS that perform logical isolation for a Medium Impact BCS	Implement for applicable systems as follows: **1.2.1.** Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability. **1.2.2.** Permit only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating all other communications. **1.2.3.** Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems that enforce access control and logical isolation such as: - Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment) - Physically isolated out-of-band network for dedicated Management Interfaces, Management Modules, or Management Systems - SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BCS and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS connected to a network via routable protocol and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI connected to a network via routable protocol hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS	Protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of: • confidentiality and integrity controls (such as encryption), or • Physical controls that restrict access to the cabling and other nonprogrammable communication components, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	Evidence may include, but is not limited to, architecture documents detailing the methods used to protect the confidentiality and integrity of the data (e.g., encryption).

CIP-005-8 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI with Dial-up Connectivity hosting High or Medium Impact BCS or their associated: • PCS; • PACS; or • EACMS	Perform authentication when establishing Dial-up Connectivity with applicable systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-8 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BCS and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS at Control Centers and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PCA; • PACS, or • EACMS	Detect known or suspected malicious Internet Protocol (IP) communications entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. For all remote access that does not originate from applicable systems in Requirement R1 Part 1.1 or Part 1.2.2, excluding Dial-up Connectivity and TCAs, the Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: • PCA Medium Impact BCS with Interactive Remote Access (IRA) and their associated: • PCA SCI with IRA hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS	Ensure that IRA is through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, or Management Systems reports that show all IRA is through an Intermediate System.

CIP-005-8 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.2	Intermediate Systems used to access applicable systems of Part 2.1	Protect the confidentiality and integrity (e.g., encryption) of IRA between the client and the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where confidentiality and integrity controls initiate and terminate.
2.3	Intermediate Systems used to access applicable systems of Part 2.1	Require multi-factor authentication to the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BCS with vendor remote access and their associated: • PCA Medium Impact BCS with vendor remote access and their associated: • PCA SCI with vendor remote access hosting High or Medium Impact BCS or their associated: • PCA Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including IRA and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BCS with vendor remote access and their associated: • PCA Medium Impact BCS with vendor remote access and their associated: • PCA SCI with vendor remote access hosting High or Medium Impact BCS or their associated: • PCA Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including IRA and system-to-system remote access.

CIP-005-8 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.6	Intermediate Systems used to access applicable systems of Part 2.1	Implement for applicable systems as follows: **2.6.1.** Restrict Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI. **2.6.2.** Permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Configuration showing that the CPU and memory can only be shared with other IS. • Configuration showing how communications are controlled between the IS and applicable systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BCS EACMS and PACS associated with Medium Impact BCS with External Routable Connectivity (ERC) SCI hosting EACMS or PACS associated with High or Medium impact BCS Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BCS EACMS and PACS associated with Medium Impact BCS with ERC SCI hosting EACMS or PACS associated with High or Medium impact BCS	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS		active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. **Compliance Monitoring Process**

1.1. **Compliance Enforcement Authority:** "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R1 – Logical Isolation*. (Requirement R1) OR The Responsible Entity did not permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. (Requirement R1 Part 1.1) OR The Responsible Entity did not implement, for applicable systems, a method for restricting Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				capability (Requirement R1 Part 1.2.1) OR The Responsible Entity did not implement, for applicable systems, a method for permitting only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating all other communications. (Requirement R1 Part 1.2.2) OR The Responsible Entity did not implement, for applicable systems, a method for denying communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability (Requirement R1 Part 1.2.3) OR

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				The Responsible Entity did not implement a method to protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of confidentiality and integrity controls (such as encryption); or physical controls that restrict access to the cabling and other nonprogrammable communication components (Requirement R1 Part 1.3) OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the applicable systems. (Requirement R1 Part 1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for	The Responsible Entity did not implement processes for one of the applicable	The Responsible Entity did not implement processes for two of the applicable	The Responsible Entity did not implement processes for three of the applicable

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement Parts 2.1 through 2.3.	items for Requirement Parts 2.1 through 2.3.	items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Requirement R2 Part 2.4); or one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (Requirement R2 Part 2.5).	items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Requirement R2 Part 2.4) and one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (Requirement R2 Part 2.5). OR The Responsible Entity did not implement a method for applicable systems restricting Intermediate Systems to only share CPU and memory with its associated SCI and other Intermediate Systems, per

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				system capability (Requirement R2 Part 2.6.1) OR The Responsible Entity did not implement a method for applicable systems permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1 (Requirement R2 Part 2.6.2).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS, SCI, and Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS, SCI and Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote	The Responsible Entity did not implement any processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Part 3.2 for EACMS, SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.2).	connections for EACMS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS, SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (Requirement R3 Part 3.2). OR The Responsible Entity had method(s) as required by Part 3.1 for PACS and EACMS but did not have a method to determine authenticated vendor-initiated remote connections for SCI or Management Modules of SCI (Requirement R3 Part 3.1).	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity had method(s) as required by Part 3.2 for PACS and EACMS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI or management Modules of SCI (Requirement R3 Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.”
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	
8	TBD	Virtualization modifications and ERC/IRA	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System -Logical Isolation~~Electronic Security Perimeter(s)~~

2. **Number:** CIP-005-8~~7~~

3. **Purpose:** To ~~manage electronic access to~~protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to and from the system and logically isolating all other communication~~.by specifying a controlled Electronic Security Perimeter~~ to reduce the likelihood of misoperations or instability in the BES. ~~in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.~~

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and

including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8~~7~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters~~logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber ~~S~~systems associated with communication links between Cyber Assets, ~~or~~ Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Date: See Project 2016-02 Virtualization Implementation Plan. ~~for Project 2019-03.~~

~~**Background:** Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its~~

~~documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~

~~**High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.~~

~~**High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~

~~**Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.~~

~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact ~~BES Cyber Systems~~BCS connected to a network via a routable protocol and their associated: 1. Protected Cyber Asset (PCA); ~~1.~~2. Physical Access Control Systems (PACS) hosted on SCI; and ~~2.~~3. Electronic Access Control or Monitoring System (EACMS) hosted on SCI Medium Impact ~~BES Cyber Systems~~BCS connected to a network via a routable protocol and their associated: 1. PCA; ~~1.~~2. PACS hosted on SCI; and ~~2.~~3. EACMS hosted on SCI	~~All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP~~ Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	~~An e~~Examples of evidence may include, but is not limited to, ~~a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP~~documentation that includes the configuration of systems ~~that enforce electronic access control and logical isolation and document business need~~ such as: • Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • SCI configuration or policies (hypervisor, fabric, backplane, or SAN configuration);~~.~~ that enforces electronic access control and logical isolation and documents the business need.

CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation

Part	Applicable Systems	Requirements	Measures
1.2	SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS EACMS that perform logical isolation for a High Impact BCS EACMS that perform logical isolation for a Medium Impact BCS ~~High Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~	~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~ Implement for applicable systems as follows: **1.2.1.** Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability. **1.2.2.** Permit only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating all other communications. **1.2.3.** Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.	~~An e~~Examples of evidence may include, but is not limited to, ~~network diagrams showing all external routable communication paths and the identified EAPs~~documentation that includes the configuration of systems that enforce access control and logical isolation such as: • Logically isolated out-of-band network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment) • Physically isolated out-of-band network for dedicated Management Interfaces, Management Modules, or Management Systems • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8~~7~~ Table R1 – ~~Electronic Security Perimeter~~Logical Isolation

Part	Applicable Systems	Requirements	Measures
1.3	High Impact BCS and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS connected to a network via routable protocol and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI connected to a network via routable protocol hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	Protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of: • confidentiality and integrity controls (such as encryption), or • Physical controls that restrict access to the cabling and other nonprogrammable communication components, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE). ~~Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.~~	~~An example of e~~Evidence may include, but is not limited to, architecture documents detailing the methods used to protect the confidentiality and integrity of the data (e.g., encryption)~~a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason~~.

CIP-005-~~8~~7 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact ~~BES Cyber Systems~~BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and ~~1.~~3. EACMS hosted on SCI Medium Impact ~~BES Cyber Systems~~BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI with Dial-up Connectivity hosting High or Medium Impact BCS or their associated: • PCS; • PACS; or • EACMS	~~Where technically feasible, p~~Perform authentication when establishing Dial-up Connectivity with applicable ~~Cyber Assets~~systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-~~8~~7 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BCS and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS at Control Centers and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PCA; • PACS, or • EACMS ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers~~	~~Have one or more methods for~~ D~~d~~etect~~ing~~ known or suspected malicious Internet Protocol (IP) communications ~~for both inbound and outbound communications~~entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. For all remote access that does not originate from applicable systems in Requirement R1 Part 1.1 or Part 1.2.2, excluding Dial-up Connectivity and TCAs, the ~~Each~~ Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, ~~where technically feasible~~per system capability, in *CIP-005-8~~7~~ Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8~~7~~ Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~Interactive Remote Access (IRA) and their associated: • PCA SCI with IRA hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS~~.~~ Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS	Ensure that ~~authorized~~ IRA is through an Intermediate System. ~~For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~	Examples of evidence may include, but are not limited to, network diagrams, ~~or~~ architecture documents, or Management Systems reports that show all IRA is through an Intermediate System.
2.2	Intermediate Systems used to access applicable systems of Part 2.1	Protect the confidentiality and integrity (e.g., encryption) of IRA between the client and the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where ~~encryption~~ confidentiality and

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~High Impact BES Cyber Systems and their associated:~~ ~~1. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~	~~For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.~~	integrity controls initiate~~s~~ and terminate~~s~~.
2.3	Intermediate Systems used to access applicable systems of Part 2.1 ~~High Impact BES Cyber Systems and their associated:~~ ~~2. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~3. PCA~~	Require multi-factor authentication ~~for all Interactive Remote Access sessions~~to the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-~~8~~7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact ~~BES Cyber Systems~~BCS with vendor remote access and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with vendor remote access ~~External Routable Connectivity~~ and their associated: • PCA SCI with vendor remote access hosting High or Medium Impact BCS or their associated: • PCA Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-~~8~~7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact ~~BES Cyber Systems~~BCS with vendor remote access and their associated: - PCA Medium Impact ~~BES Cyber Systems~~BCS with vendor remote access~~External Routable Connectivity~~ and their associated: - PCA SCI with vendor remote access hosting High or Medium Impact BCS or their associated: - PCA Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated: - PCA	Have one or more method(s) to disable active vendor remote access (including ~~Interactive Remote Access~~ IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including ~~Interactive Remote Access~~ IRA and system-to-system remote access.~~),such as:Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Intermediate Systems used to access applicable systems of Part 2.1	Implement for applicable systems as follows: **2.6.1.** Restrict Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI. **2.6.2.** Permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1.	Examples of evidence may include, but is not limited to, documentation that includes the following: • Configuration showing that the CPU and memory can only be shared with other IS. • Configuration showing how communications are controlled between the IS and applicable systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-~~7~~ 8 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~7~~ 8 Table R3 – Vendor Remote Access Management for EACMS and PACS* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact ~~BES Cyber Systems~~BCS EACMS and PACS associated with Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity (ERC) SCI hosting EACMS or PACS associated with High or Medium impact BCS Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact ~~BES Cyber Systems~~BCS EACMS and PACS associated with Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable~~	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include

CIP-005-~~8~~7 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	Applicable Systems	Requirements	Measures
	~~Connectivity~~ERC SCI hosting EACMS or PACS associated with High or Medium impact BCS Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS		terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.~~for both inbound and outbound communications. (1.5)~~	The Responsible Entity did not document one or more processes for *CIP-005-~~7~~ 8 Table R1 – ~~Electronic Security Perimeter~~Logical Isolation*. (Requirement R1) OR The Responsible Entity did not permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. ~~have all applicable Cyber Assetssystems connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). protected by logical isolation~~ (Requirement R1 Part 1.1) OR The Responsible Entity did not ~~protect~~implement, for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable systems, a method for restricting Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability ~~the Management Systems or Management Interfaces or applicable systems per Requirement R1, Part 1.2External Routable Connectivity through the ESP was not through an identified EAP.~~ (Requirement R1 Part 1.2.1) OR The Responsible Entity did not implement, for applicable systems, a method for permitting only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				all other communications. (Requirement R1 Part 1.2.2) OR The Responsible Entity did not implement, for applicable systems, a method for denying communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability (Requirement R1 Part 1.2.3) OR The Responsible Entity did not implement a method to protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of confidentiality and integrity controls (such as encryption); or physical controls that restrict access to the cabling and other

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				nonprogrammable communication components ~~-protect confidentiality and integrity of the data traversing communications links per Requirement R1, Part 1.3.The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default.~~ (Requirement R1 Part 1.3) OR The Responsible Entity did not perform authentication when establishing D~~d~~ial-up ~~c~~Connectivity with the applicable ~~Cyber Assets~~systems~~, where technically feasible~~. (Requirement R1 Part 1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3;	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3;

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement Parts 2.1 through 2.3.		OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Requirement R2 Part 2.4); or one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Requirement R2 Part 2.5).	OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Requirement R2 Part 2.4) and one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Requirement R2 Part 2.5). OR The Responsible Entity did not implement a method for applicable systems restricting Intermediate Systems to only share CPU and memory with its associated SCI and other Intermediate Systems, per

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				system capability (Requirement R2 Part 2.6.1) OR The Responsible Entity did not implement a method for applicable systems permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1 (Requirement R2 Part 2.6.2).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS,~~ and~~ SCI, and -Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS,~~ and~~ SCI and Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote	The Responsible Entity did not implement any processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Part 3.2 for EACMS,~~ and~~ SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.2).	connections for EACMS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS,~~ and~~ SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (Requirement R3 Part 3.2). OR The Responsible Entity had method(s) as required by Part 3.1 for PACS and ~~and~~ EACMS but did not have a method to determine authenticated vendor-initiated remote connections for SCI or Management Modules of SCI (Requirement R3 Part 3.1).	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity had method(s) as required by Part 3.2 for PACS and EACMS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI or management Modules of SCI (Requirement R3 Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.” ~~for Project 2019-03~~
- CIP-005-8~~7~~ Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	
8	TBD	Virtualization modifications and ERC/IRA	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-7:

4.2.3.1 Cyber systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Dates: See "Project 2016-02 Virtualization Implementation Plan"

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BCS without External Routable Connectivity (ERC) SCI without ERC hosting Medium Impact BCS Physical Access Control Systems (PACS) associated with: • High Impact BCS • Medium Impact BCS with ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI with ERC hosting Medium Impact BCS or their associated: - EACMS; or - PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: - EACMS; or - PCA	Utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, per system capability.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-7 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.5	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: - EACMS; or - PCA SCI with ERC hosting Medium Impact BCS or their associated: - EACMS; or - PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident response plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

CIP-006-7 Table R1– Physical Security Plan			
Part	Applicable Systems	Requirements	Measures
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BCS • Medium Impact BCS with ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BCS • Medium Impact BCS with ERC • SCI hosting High Impact BCS or their associated EACMS or PCAs; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident response plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated • EACMS; or • PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.1	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: - EACMS; or - PCA SCI with ERC hosting Medium Impact BCS or their associated: - EACMS; or - PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with EERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BCS • Medium Impact BCS with ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BCS • Medium Impact BCS with ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Requirement R1 Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Requirement R1 Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Requirement R1 Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (Requirement R1 Part 1.4)

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (Requirement R1 Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (Requirement Part 1.8) OR The Responsible Entity does not have a process

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				to retain physical access logs for 90 calendar days. (Requirement R1 Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Requirement R2 Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Requirement R2 Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (Requirement R2 Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (Requirement R3 Part 3.1) OR The Responsible Entity has documented and

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Requirement R3 Part 3.1)	hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Requirement R3 Part 3.1)	devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Requirement R3 Part 3.1)	implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (Requirement R3 Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Virtualization Implementation Plan”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of	Addressed FERC

Version	Date	Action	Change Tracking
		Trustees.	directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes and CEC language added	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. Title: Cyber Security — Physical Security of BES Cyber Systems

2. Number: CIP-006-7~~6~~

3. Purpose: To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~**4.1.6**~~**4.1.5 Reliability Coordinator**

~~**4.1.7**~~**4.1.6 Transmission Operator**

~~**4.1.8**~~**4.1.7 Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-7~~6~~:

4.2.3.1 Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters~~logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

~~**4.2.3.2**~~**4.2.3.3** Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets (VCA), or SCI performing logical isolation that extends to one or more geographic locations.

~~**4.2.3.3**~~**4.2.3.4** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4**~~**4.2.3.5** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.5**~~**4.2.3.6** Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. **Effective Dates:** See "Project 2016-02 Virtualization Implementation Plan"

~~**6. Background:**~~

~~Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**"Applicable Systems" Columns in Tables:**~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.~~

~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Locally mounted hardware or devices at the Physical Security Perimeter** – Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7~~6~~ Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7~~6~~ Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.1	Medium Impact ~~BES Cyber Systems~~BCS without External Routable Connectivity (ERC) SCI without ERC hosting Medium Impact BCS Physical Access Control Systems (PACS) associated with: • High Impact BCS~~BES Cyber Systems, or~~ • Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-7~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.2	Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI with ERC hosting Medium Impact BCS or their associated: - EACMS; or - PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: - EACMS; or - PCA	~~Where technically feasible, u~~Utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, per system capability.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: - EACMS; or - PCA SCI with ERC hosting Medium Impact BCS or their associated: - EACMS; or - PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: - EACMS; or - PCA SCI with ERC hosting Medium Impact BCS or their associated: - EACMS; or - PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident ~~R~~response ~~P~~plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

CIP-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	Physical Access Control Systems (PACS) associated with: - High Impact ~~BES Cyber Systems~~BCS~~, or~~ - Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC - SCI hosting High Impact BCS or their associated EACMS or PCA; or - SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact ~~BES Cyber Systems~~BCS~~, or~~ • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • SCI hosting High Impact BCS or their associated EACMS or PCAs; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident ~~R~~response ~~P~~plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: - EACMS; or - PCA SCI with ERC hosting Medium Impact BCS or their associated - EACMS; or - PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-7~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.9	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

~~CIP-006-6 Table R1 – Physical Security Plan~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~1.10~~	~~High Impact BES Cyber Systems and their associated:~~ - ~~PCA~~ ~~Medium Impact BES Cyber Systems at Control Centers and their associated:~~ - ~~PCA~~	~~Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.~~ ~~Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:~~ - ~~encryption of data that transits such cabling and components; or~~ - ~~monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or~~ - ~~an equally effective logical protection.~~	~~An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.~~

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7~~6~~ Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: - EACMS; or - PCA SCI with ERC hosting Medium Impact BCS or their associated: - EACMS; or - PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter~~, except during CIP Exceptional Circumstances~~.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-7~~6~~ Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with E~~xternal Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: • EACMS; or • PCA SCI with ERC hosting Medium Impact BCS or their associated: • EACMS; or • PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7~~6~~ Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: - EACMS; or - PCA SCI with ERC hosting Medium Impact BCS or their associated: - EACMS; or - PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7~~6~~ Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact ~~BES Cyber Systems~~BCS~~, or~~ • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact ~~BES Cyber Systems~~BCS~~, or~~ • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Requirement R1 Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Requirement R1 Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems.

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(Requirement R1 Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (Requirement R1 Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (Requirement R1 Part 1.6)

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (Requirement Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Requirement R1 Part 1.9) ~~OR~~ ~~The Responsible Entity did not document or implement physical access restrictions, encryption,~~

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)~~
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Requirement R2 Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact.

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				(Requirement R2 Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (Requirement R2 Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (Requirement R3 Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (Requirement R3 Part

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ See "Project 2016-02 Virtualization Implementation Plan"

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with

Version	Date	Action	Change Tracking
			other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes and CEC language added	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Dates:

See "Project 2016-02 Virtualization Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1* – System Hardening. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1* – System Hardening and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated: 1. EACMS 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Enable only network accessible services that have been determined to be needed by the Responsible Entity (or logical network accessible ports if unable to determine service, including port ranges where needed to handle dynamic ports), per system capability. If a system has no provision for disabling or restricting network accessible services (or logical ports) then those services (or logical ports), that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports, individually or by group. • Listings of the listening ports, individually or by group, from either configuration files, command output (such as netstat), or network scans of open ports; or • Configuration of host-based firewalls, policy, or other mechanisms that only allow needed ports and deny all others.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated PCA. Medium Impact BCS at Control Centers and their associated PCA SCI at Control Centers hosting High or Medium Impact BCS or their associated PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA Non-programmable communications components within a PSP that are not logically isolated from High or Medium impact BCS at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Enable only services that have been determined to be needed by the Responsible Entity, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of implemented hardening guidelines • Configuration management reporting that demonstrates the need for all enabled services.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for systems that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: - Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or - A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Protection [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, white-listing, privileged introspection, etc.).

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BCS is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High or Medium Impact BCS or their associated: • PACS • EACMS; or • PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, at a minimum, each of the following types of events, per system capability: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
4.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers hosting High Impact BCS, Medium Impact BCS, or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: - EACMS; or - PCA Management Modules of SCI hosting High BCS or their associated: - EACMS; or - PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS, or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI at	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Control Centers hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA		
5.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use.

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS, Medium Impact BCS, or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS, or their associated • PACS; • EACMS; or • PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Change known default passwords, per system capability.	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the system; and 5.5.2 Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the system.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS, Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity has implemented and documented processes for System Hardening but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Requirement R1 Part 1.2)	The Responsible Entity has implemented and documented processes for determining necessary System Hardening, but had one or more unneeded network accessible services enabled. (Requirement R1 Part 1.1) OR The Responsible Entity has implemented and documented processes for determining necessary System Hardening, but had one or more unneeded services enabled. (Requirement R1 Part 1.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)
R2	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	patches for applicable systems. (Requirement R2 Part 2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation	patches for applicable systems. (Requirement R2 Part 2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,	Table R2. (Requirement R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable systems. (Requirement R2 Part 2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		completion. (Requirement R2 Part 2.3)	did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	delegate. (Requirement R2 Part 2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (Requirement R2 Part 2.4)
R3	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Requirement R3 Part 3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (Requirement R3 Part 3.2) OR The Responsible Entity has implemented one or more	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R3. (Requirement R3). OR

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-007-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td>documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Requirement R3 Part 3.3).</td><td>The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (Requirement R3 Part 3.1)</td></tr>
<tr><td>**R4**</td><td>The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (Requirement R4 Part 4.4)</td><td>The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (Requirement R4 Part 4.4)</td><td>The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (Requirement R4 Part 4.2)
OR</td><td>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R4. (Requirement R4)
OR
The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system</td></tr>
</table>

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (Requirement R4 Part 4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (Requirement R4 Part 4.4)	capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Requirement R4 Part 4.1)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R5	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Requirement R5 Part 5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Requirement R5 Part 5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (Requirement R5 Part 5.3) OR The Responsible Entity has implemented one or more	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R5. (Requirement R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more documented process(es) for System

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more	Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords. (Requirement R5 Part 5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Requirement R5 Part 5.6)	authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See Project 2016-02 Virtualization Implementation Plan.
- See Technical Rationale for CIP-007-7

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	

Version	Date	Action	Change Tracking
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	TBD	Virtualization modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7~~6~~

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

~~4.1.4~~ Generator Owner

~~4.1.5~~4.1.4 ~~Interchange Coordinator or Interchange Authority~~

~~4.1.6~~4.1.5 Reliability Coordinator

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-007-~~6~~7:

4.2.3.1 Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~ systems associated with ~~communication networks and data~~ communication links ~~between discrete~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI). ~~Electronic Security Perimeters.~~

4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.2~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.3~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Dates:

See "Project 2016-02 Virtualization Implementation Plan." ~~for CIP-007-~~7~~6).~~

~~6. Background:~~

~~Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training~~

~~program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~“Applicable Systems” Columns in Tables:~~

~~Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~

~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ 7 Table R1 –* System Hardening~~*Ports and Services*~~. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~ 7 Table R1 –* System Hardening~~*Ports and Services*~~ and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	~~Where technically feasible, ~~E~~e~~nable only ~~logical~~ network accessible ~~ports~~ services that have been determined to be needed by the Responsible Entity~~,~~ (or logical network accessible ports if unable to determine service, including port ranges ~~or services~~ where needed to handle dynamic ports), per system capability. -If a ~~device~~ system has no provision for disabling or restricting network accessible services (or logical ports) ~~on the device~~ then those ~~ports~~ services (or logical ports), that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports, ~~on all applicable Cyber Assets and Electronic Access Points,~~ individually or by group. • Listings of the listening ports, ~~on the Cyber Assets,~~ individually or by group, from either ~~the device~~ configuration files, command output (such as netstat), or network scans of open ports; or • Configuration ~~files~~ of host-based firewalls,~~-~~ policy, or other ~~device level~~ mechanisms that only allow needed ports and deny all others.

1.2	High Impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ PCA.~~; and~~ ~~1. Nonprogrammable communication components located inside both a PSP and an ESP.~~ Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated ~~:~~PCA ~~; and~~ ~~1. Nonprogrammable communication components located inside both a PSP and an ESP.~~ SCI at Control Centers hosting High or Medium Impact BCS or their associated PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA Non-programmable communications components within a PSP that are not logically isolated from High or Medium impact BCS at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
	SCI hosting High or Medium Impact BCS or their associated:	Enable only services that have been determined to be needed by the	Examples of evidence may include, but are not limited to:

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	• PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Responsible Entity, per system capability.	• Documentation of implemented hardening guidelines • Configuration management reporting that demonstrates the need for all enabled services.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	A patch management process for tracking, evaluating, and installing cyber security patches. ~~for applicable Cyber Assets.~~ The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for systems ~~for applicable Cyber Assets~~ that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored~~, whether on an individual BES Cyber System or Cyber Asset basis.~~ .

CIP-007-7~~6~~ Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA~~; and~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA~~; and~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-7~~6~~ Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; ~~or~~ • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-7~~6~~ Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES ~~-~~Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R3 – Malicious Code Protection~~Prevention.~~* *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R3 – Malicious Code Protection~~Prevention~~* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R3 – Malicious Code Protection~~Prevention~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, white-listing, privileged introspection, etc.).

CIP-007-7~~6~~ Table R3 – Malicious Code Protection~~Prevention~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-7~~6~~ Table R3 – Malicious Code Protection~~Prevention~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Log security events, per system capability, ~~at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Aasset level (per Cyber Aasset capability)~~ for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, at~~s~~ a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the ~~BES Cyber System~~ BCS is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

4.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS or Medium Impact BCS ~~with ERC~~ or their associated: - PACS; - EACMS; or - PCA Management Modules with ERC of SCI hosting High or Medium Impact BCS or their associated: - PACS - EACMS; or - PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, a~~s~~t a minimum, each of the following types of events, ~~(~~per system ~~or Cyber Aasset or BES Cyber System~~ capability~~)~~:~~:~~ 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

4.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers hosting High Impact BCS, Medium Impact BCS, or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	~~Where technically feasible, r~~Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system ~~or asset~~ capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.

CIP-007-7~~6~~ Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BCS or their associated: - EACMS; or - PCA Management Modules of SCI hosting High BCS or their associated: - EACMS; or - PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity (ERC) and their associated:	Have a method(s) to enforce authentication of interactive user access, per system capability~~where technically feasible~~.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~6~~7 Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
	1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS, or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA		
5.2	High Impact ~~BES Cyber Systems~~BCS and their associated:	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use~~ for the BES Cyber System~~.

CIP-007-~~6~~7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA		

CIP-007-7~~6~~ Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
5.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS, Medium Impact BCS, or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS, or their associated • PACS; • EACMS; or • PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Change known default passwords, per system ~~or Cyber Aasset~~ capability.	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique~~ to the device~~.

CIP-007-7~~6~~ Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the system~~Cyber Asset~~; and 5.5.2 Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the system.~~Cyber Asset.~~	Examples of evidence may include, but are not limited to: - System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or - Attestations that include a reference to the documented procedures that were followed.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI with ERC hosting High Impact BCS, Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS or their associated: • PACS;	~~Where technically feasible, F~~For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

	- EACMS; or - PCA		

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS or their associated:	~~Where technically feasible, either:~~ Limit the number of unsuccessful authentication attempts~~;~~ or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: - Documentation of the account lockout parameters; or - Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

	• PACS; • EACMS; or • PCA Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA		

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~1.3. Compliance Monitoring and Assessment Processes:~~

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

~~Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	N/A	The Responsible Entity has implemented and documented processes for ~~Ports and Services~~ System Hardening but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Requirement R1 Part 1.2)	The Responsible Entity has implemented and documented processes for determining necessary System Hardening~~Ports and Services but~~, ~~where technically feasible,~~ but had one or more unneeded ~~logical~~ network accessible services ~~ports~~ enabled. (Requirement R1 Part 1.1) OR The Responsible Entity has implemented and documented processes for determining necessary System Hardening, but had one or more unneeded services enabled. (Requirement R1 Part 1.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7~~6~~ Table R1. (Requirement R1)
R2	The Responsible Entity has documented and implemented one or more	The Responsible Entity has documented or implemented one or more process(es) for patch	The Responsible Entity has documented or implemented one or more	The Responsible Entity did not implement or document one or more

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar	management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable ~~Cyber Assets~~systems. (Requirement R2 Part 2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not	process(es) for patch management but did not include any processes for installing cyber security patches for applicable ~~Cyber Assets~~ systems. (Requirement R2 Part 2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating	process(es) that included the applicable items in CIP-007-7~~6~~ Table R2. (Requirement R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable ~~Cyber Assets~~systems. (Requirement R2 Part 2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	days of the evaluation completion. (Requirement R2 Part 2.3)	apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate. (Requirement R2 Part 2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (Requirement R2 Part 2.4)
R3	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the	The Responsible Entity did not implement or document one or more process(es) that

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		used, the Responsible Entity did not address testing the signatures or patterns. (Requirement R3 Part 3.3)	threat of detected malicious code. (Requirement R3 Part 3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Requirement R3 Part 3.3).	included the applicable items in CIP-007-7~~6~~ Table R3. (Requirement R3). OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (Requirement R3 Part 3.1)
R4	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7~~6~~ Table R4. (Requirement R4)

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (Requirement R4 Part 4.4)	calendar days of the prior review. (Requirement R4 Part 4.4)	but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (Requirement R4 Part 4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (~~where technically feasible and~~ except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (Requirement R4 Part 4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an	OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Requirement R4 Part 4.1)

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (Requirement R4 Part 4.4)	
R5	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Requirement R5 Part 5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Requirement R5 Part 5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7~~6~~ Table R5. (Requirement R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access.

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			identification of the individuals with authorized access to shared accounts. (Requirement R5 Part 5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of	(Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords.

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-007-7~~6~~)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td>the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5)
OR
The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Requirement R5 Part 5.6)</td><td>(Requirement R5 Part 5.4)
OR
The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5)
OR
The Responsible Entity has implemented one or more documented process(es) for password-only authentication for</td></tr>
</table>

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but~~, where technically feasible~~, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- ~~None.~~See Project 2016-02 Virtualization Implementation Plan.
- See Technical Rationale for CIP-007-7

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	TBD	Virtualization modifications	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.~~

~~**1.1.** This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'~~

~~1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.~~

~~The protection of these ports can be accomplished in several ways including, but not limited to:~~

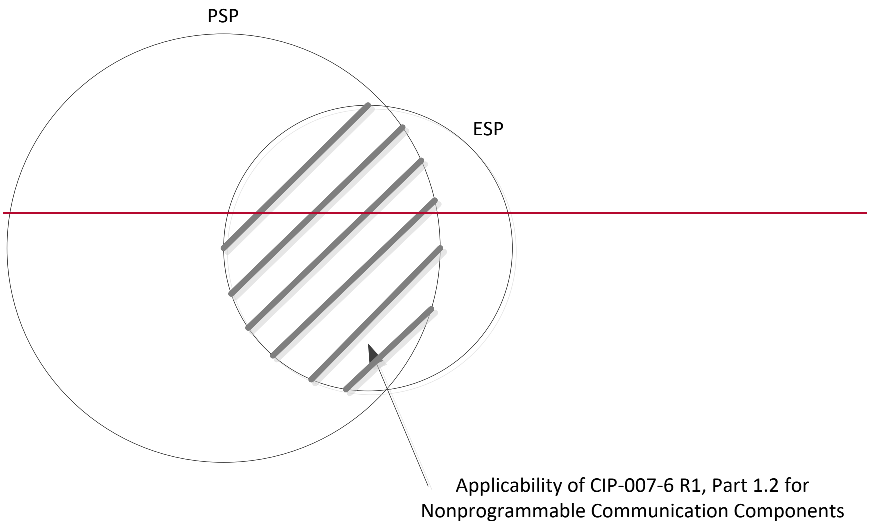
- ~~Disabling all unneeded physical ports within the Cyber Asset's configuration~~
- ~~Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization~~
- ~~Physical port obstruction through removable locks~~

~~The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.~~

~~This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.~~

~~The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:~~

Location of Nonprogrammable Communication Components



~~**Requirement R2:**~~

~~The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.~~

~~Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.~~

~~One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.~~

~~**2.1.** The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they~~

~~can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.~~

~~**2.2.** Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.~~

~~When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.~~

~~**2.3.** The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or~~

~~those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.~~

~~**2.4.** The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.~~

~~**Requirement R3:**~~

~~**3.1.** Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.~~

~~**3.2.** When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or~~

~~method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.~~

~~Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.~~

~~**3.3.** In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.~~

~~**Requirement R4:**~~

~~Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.~~

~~**4.1.** In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.~~

~~Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.~~

~~User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.~~

~~It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.~~

~~**4.2.** Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.~~

~~The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:~~

- ~~Detected known or potential malware or malicious activity~~
- ~~Failure of security event logging mechanisms~~
- ~~Login failures for critical accounts~~
- ~~Interactive login of system accounts~~
- ~~Enabling of accounts~~
- ~~Newly provisioned accounts~~
- ~~System administration or change tasks by an unauthorized user~~
- ~~Authentication attempts on certain accounts during non-business hours~~
- ~~Unauthorized configuration changes~~
- ~~Insertion of Removable Media in violation of a policy~~

~~**4.3** Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.~~

~~**4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-~~

~~time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.~~

~~**Requirement R5:**~~

~~Account types referenced in this guidance typically include:~~

- ~~Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.~~
- ~~Individual user account: An account used by a single user.~~
- ~~Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.~~
- ~~System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.~~
- ~~Application account: A specific system account, with rights granted at the application level often used for access into a Database.~~
- ~~Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.~~
- ~~Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.~~
- ~~Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.~~

~~**5.1** Reference the Requirement's rationale.~~

~~**5.2** Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.~~

~~**5.3** Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.~~

~~**5.4.** Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.~~

~~The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.~~

~~**5.5.** Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.~~

~~Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.~~

~~**5.6** Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.~~

~~**5.7** Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.~~

~~Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.~~

~~In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.~~

~~The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).~~

~~Rationale for Requirement R2:~~

~~Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.~~

~~Rationale for Requirement R3:~~

~~Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.~~

~~Rationale for Requirement R4:~~

~~Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.~~

~~Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.~~

~~Rationale for Requirement R5:~~

~~To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.~~

~~Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.~~

~~Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.~~

~~Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.~~

~~For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.~~

~~The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.~~

~~The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.~~

~~The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.~~

~~Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard being posted for a 5-day final ballot period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-7:

4.2.3.1 Cyber systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BCS) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Dates:

See “Project 2016-02 Virtualization Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS.	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the “Applicable Systems” column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column including justification for attempt determination criteria and documented processes for notification.
1.3	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS and their associated: • EACMS Medium ImpactBCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations-based exercises.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: - EACMS Medium Impact BCS and their associated: - EACMS SCI hosting High or Medium Impact BCS or their associated: - EACMS	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact BCS and their associated: - EACMS Medium Impact BCS and their associated: - EACMS SCI hosting High or Medium Impact BCS or their associated: - EACMS	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: - EACMS Medium Impact BCS and their associated: - EACMS SCI hosting High or Medium Impact BCS or their associated: - EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC),[1] or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

---

[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.
4.3	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Requirement R1 Part 1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (Requirement R1 Part 1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Requirement R1 Part 1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (Requirement R1 Part 1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (Requirement R1 Part 1.2)	from Part 1.2.1, a system identified in the "Applicable Systems" column for Part 1.2. (Requirement R1 Part 1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months, not exceeding 16 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 17 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 18 calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.2 occurs. (Requirement R2 Part 2.2)	calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.3. (Requirement R2 Part 2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security	The Responsible Entity has not updated the Cyber Security Incident response plan based on any	The Responsible Entity has neither documented lessons learned nor documented the	The Responsible Entity has neither documented lessons learned nor documented the

<table>
<tr><th rowspan="2">R #</th><th rowspan="2">Time Horizon</th><th rowspan="2">VRF</th><th colspan="4">Violation Severity Levels (CIP-008-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td>Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3)</td><td>documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2)
OR
The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3)
OR</td><td>absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1)
OR
The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2)
OR
The Responsible Entity has not updated the Cyber Security</td><td>absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1)</td></tr>
</table>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their	The Responsible Entity failed to notify E-ISAC or NCCIC, or their	The Responsible Entity notified E-ISAC and NCCIC, or their	The Responsible Entity failed to notify E-ISAC and NCCIC, or their

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3	successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column. (Requirement R4 Part R4)	successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Requirement R4 Part 4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1.			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Requirement R4 Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Virtualization Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	

Version	Date	Action	Change Tracking
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard being posted for a 5-day final ballot period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7~~6~~

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1 Balancing Authority

    4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3 Generator Operator

    4.1.4 Generator Owner

    4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-7~~6~~:

4.2.3.1 Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete~~

~~Electronic Security Perimeters~~logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

~~4.2.3.2~~4.2.3.3 Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BCS) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. Effective Dates:

See “Project 2016-02 Virtualization Implementation Plan.” ~~for CIP-008-76.~~

~~6. Background:~~

~~Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.~~

~~An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS.	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the “Applicable Systems” column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column including justification for attempt determination criteria and documented processes for notification.
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.4	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations-~~-~~based exercises.

CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS SCI hosting High or Medium Impact BCS or their associated: - EACMS	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the “Applicable Systems” column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS SCI hosting High or Medium Impact BCS or their associated: - EACMS	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the “Applicable Systems” column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, ~~all of~~ the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC),[1] or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and NCCIC.

---

[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.

CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact ~~BES Cyber Systems~~BCS and their associated: • EACMS Medium Impact ~~BES Cyber Systems~~ BCS and their associated: • EACMS SCI hosting High or Medium Impact BCS or their associated: • EACMS	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and NCCIC.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Assessment~~ Enforcement Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~
- ~~Complaint~~

~~1.4. Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Requirement R1 Part 1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (Requirement R1 Part 1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Requirement R1 Part 1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (Requirement R1 Part 1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (Requirement R1 Part 1.2)	from Part 1.2.1, a system identified in the "Applicable Systems" column for Part 1.2. (Requirement R1 Part 1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			calendar months, not exceeding 16 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 17 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 18 calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.2 occurs. (Requirement R2 Part 2.2)	calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.3. (Requirement R2 Part 2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security	The Responsible Entity has not updated the Cyber Security Incident response plan based on any	The Responsible Entity has neither documented lessons learned nor documented the	The Responsible Entity has neither documented lessons learned nor documented the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3)	documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3) OR	absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the Cyber Security	absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) - Roles or responsibilities, or - Cyber Security Incident response groups or individuals, or - Technology changes.	Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) - Roles or responsibilities, or - Cyber Security Incident response groups or individuals, or - Technology changes.	
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Cyber	The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Cyber	The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a	The Responsible Entity failed to notify E-ISAC and NCCIC, or their successors, of a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on	Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column. (Requirement R4 Part R4)	Reportable Cyber Security Incident but failed to notify or update E-ISAC or NCCIC, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	Reportable Cyber Security Incident. (Requirement R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Requirement R4 Part 4.3) OR The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1.			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7~~6~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Requirement R4 Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ See “Project 2016-02 Virtualization Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1. **Balancing Authority**

      4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

            4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

      4.1.3. **Generator Operator**

      4.1.4. **Generator Owner**

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-009-7:

4.2.3.1. Cyber systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-7 identification and categorization processes.

4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. **Effective Dates:** See “Project 2016-02 Virtualization Implementation Plan”

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	One or more processes for the backup and storage of information required to recover applicable system functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover applicable system functionality.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BBCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	Test a representative sample of information used to recover applicable system functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover applicable system functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BCS SCI hosting High Impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: 1. PACS: and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BSC at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. **Compliance Enforcement Authority:**
   As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. **Evidence Retention:**
   The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for applicable systems. OR The Responsible Entity has created recovery plan(s) for applicable systems, but the plan(s) does not address the conditions for activation in Requirement R1 Part 1.1. OR The Responsible Entity has created recovery plan(s) for applicable systems, but the plan(s) does not address three or more of the requirements in Parts Requirement R11.2 through 1.5.
R2.	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (Requirement R2 Part 2.1)	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 18

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-009-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>OR
The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Requirement R2 Part 2.2)
OR
The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Requirement R2 Part 2.3)</td><td>used in the recovery of applicable system functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Requirement R2 Part 2.2)
OR
The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Requirement R2 Part 2.3)</td><td>The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Requirement R2 Part 2.2)
OR
The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Requirement R2 Part 2.3)</td><td>calendar months between tests. (Requirement R2 Part 2.2)
OR
The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (Requirement R2 Part 2.3)</td></tr>
</table>

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Virtualization Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	

Version	Date	Action	Change Tracking
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7~~6~~

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. **Balancing Authority**

4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. **Generator Operator**

4.1.4. Generator Owner

~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

~~**4.1.6.**~~**4.1.5. Reliability Coordinator**

~~**4.1.7.**~~**4.1.6. Transmission Operator**

~~**4.1.8.**~~**4.1.7. Transmission Owner**

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~Special Protection System or Remedial Action Scheme~~RAS where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-009-7~~6~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters~~logically isolated from, but not providing logical isolation for, BES Cyber Systems or Shared Cyber Infrastructure (SCI).

~~**4.2.3.2.**~~**4.2.3.3.** Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-7~~5.1~~ identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. **Effective Dates:** See "Project 2016-02 Virtualization Implementation Plan" ~~for CIP-009-~~7~~6.~~

~~6. **Background:** Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.~~

~~An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**"Applicable Systems" Columns in Tables:**~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications*.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	One or more processes for the backup and storage of information required to recover ~~BES Cyber System~~applicable system functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover ~~BES Cyber System~~ applicable system functionality.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~ BCS at Control Centers and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS or their associated: • PACS; or • EACMS	One or more processes to preserve data, per ~~Cyber Asset~~system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact B~~ES Cyber Systems~~BCS at Control Centers and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	Test a representative sample of information used to recover ~~BES Cyber System~~applicable system- functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover ~~BES Cyber System~~applicable system functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact ~~BES Cyber Systems~~BCS SCI hosting High Impact ~~BES Cyber Systems~~BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. PACS: and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ Medium Impact ~~BES Cyber Systems~~BSC at Control Centers and their associated: 1. PACS; and 2. EACMS ~~1. EACMS; and~~ ~~2. PACS~~ SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~**1.4. Compliance Monitoring and Assessment Processes:**~~

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Investigations~~
- ~~Self-Reporting~~
- ~~Complaints~~

~~**1.5. Additional Compliance Information:**~~

~~None.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for ~~BES Cyber Systems~~applicable systems. OR The Responsible Entity has created recovery plan(s) for ~~BES Cyber Systems~~applicable systems, but the plan(s) does not address the conditions for activation in Requirement R1 Part 1.1. OR The Responsible Entity has created recovery plan(s) for ~~BES Cyber Systems~~applicable systems, but the plan(s) does not address three or more of the requirements in Parts Requirement R11.2 through 1.5.

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Requirement R2 Part 2.2) OR	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~BES Cyber System~~applicable system functionality according to R2 Part 2.2 within 18 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Requirement R2 Part 2.3)	months between tests. (Requirement R2 Part 2.3)	The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Requirement R2 Part 2.3)	
R3.	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the recovery plan(s) of updates within 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2)	

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			• Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~ See “Project 2016-02 Virtualization Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~The following guidelines are available to assist in addressing the required components of a recovery plan:~~

~~NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf~~

~~National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf~~

~~Installation files and media;~~

~~Current backup tapes and any additional documented configuration settings;~~

~~Documented build or restoration procedures; and~~

~~Cross site replication storage.~~

~~For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not~~

~~required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:~~

~~Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.~~

~~Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.~~

~~Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.~~

~~Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.~~

~~The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.~~

~~For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.~~

~~Requirement R2:~~

~~A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.~~

~~A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.~~

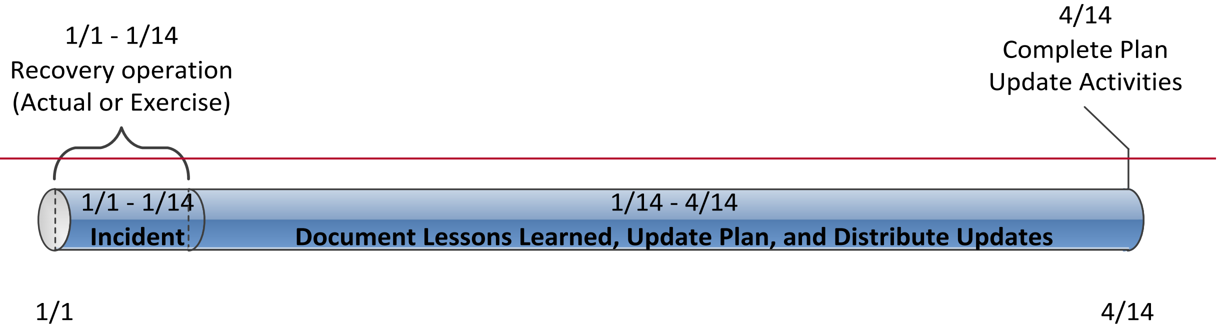
~~Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."~~

~~The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."~~

~~For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.~~

~~Requirement R3:~~
~~This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.~~

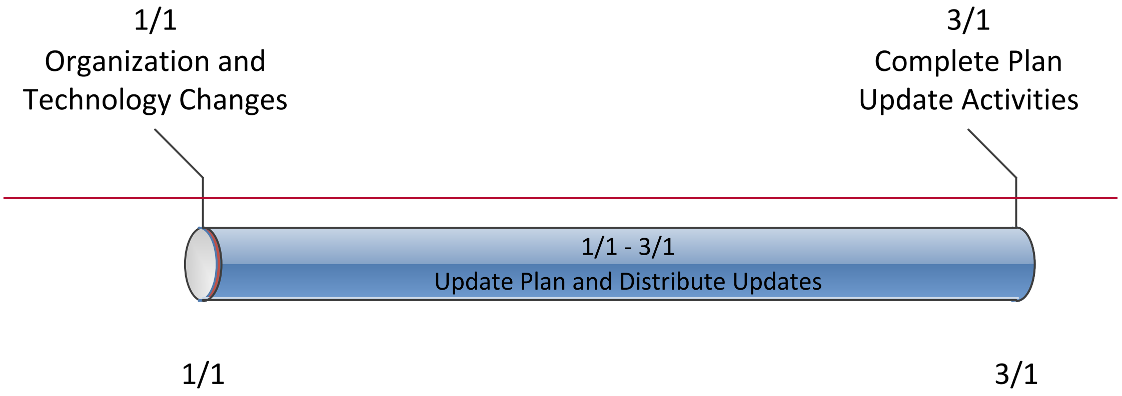
~~The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.~~



~~Figure 1: CIP-009-6 R3 Timeline~~

~~The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.~~

~~The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.~~



~~Figure 2: Timeline for Plan Changes in 3.2~~

~~When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.~~

~~Rationale for Requirement R2:~~

~~The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.~~

~~Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.~~

~~Rationale for Requirement R3:~~

~~To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of proposed standard for formal 10-day comment period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security —Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. **Effective Date:** See “Project 2016-02 Virtualization Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented change management process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 –Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 –Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Authorize changes to: 1.1.1. Operating system(s) or firmware or images used to derive operating systems or firmware; 1.1.2. Commercially available or open-source application software including Self-Contained Applications; 1.1.3. Custom software installed including Self-Contained Applications; 1.1.4. Any logical network accessible services, (or logical ports if unable to determine service); 1.1.5. Security patches applied; 1.1.6. SCI configuration that: • Enforces electronic access control that permits only	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change.

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	needed and controlled communication between systems with different impact ratings hosted on SCI; • Enforces logical isolation between systems with different impact ratings hosted on SCI; • Prevents sharing of CPU/Memory between systems with different impact ratings hosted on SCI; or • Enables or disables SCI services.	
1.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each change to the items listed in Part 1.1: 1.2.1. Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.2.2. Following the change, verify that required cyber security controls determined in 1.2.1 are not adversely affected; and 1.2.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA		
1.3	High Impact BCS SCI hosting High Impact BCS	For each change to the items listed in Part 1.1, per system capability: 1.3.1. Prior to implementing any change in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		minimizes adverse effects to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.3.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.4	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS and their associated: 1. EACMS; and 2. PACS	Prior to a change associated with Requirement Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.4.1. Verify the identity of the software source; and 1.4.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-5 Table R1 – Change Management			
Part	Applicable Systems	Requirements	Measures
	SCI hosting High or Medium Impact BCS and their associated EACMS and PACS. Management Modules of SCI hosting High or Medium Impact BCS and their associated EACMS and PACS. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.4: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.		

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Change Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Change Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Change Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for unauthorized changes to the items described in Requirement R1, Part 1.1. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems SCI hosting High Impact BCS. Management Modules of SCI hosting High Impact BCS.	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BES Cyber Systems or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High Impact BCS or their associated: • EACMS; or • PCA	Perform an active vulnerability assessment prior to logically connecting an additional applicable Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure to a production environment, per system capability, except for CIP Exceptional Circumstances, or deployments using a previously assessed configuration. The production environment does not include devices being actively remediated and logically isolated.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure) and the output of any tools or Management Systems used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a report of Management System actions, or a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated SCI and Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a change management process(es) that includes only four or more of the required items listed in 1.1.1 through 1.1.6. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a change management process(es) that includes only three of the required items listed in 1.1.1 through 1.1.6. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a change management process(es) that includes only two of the required items listed in 1.1.1 through 1.1.6. (Requirement R1 Part 1.1) OR The Responsible Entity has a process as specified in Part 1.4 to verify the identity of the software source (1.4.1) but does not have a process as specified in Part 1.4 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.4.2)	The Responsible Entity has not documented or implemented any change management process(es). (Requirement R1) OR The Responsible Entity has documented and implemented a change management process(es) that includes only one of the required items listed in 1.1.1 through 1.1.6. (Requirement R1 Part 1.1) OR The Responsible Entity does not have a change management process(es) that requires authorization of changes to items listed in 1.1.1-1.1.6. (Requirement R1 Part 1.1) OR The Responsible Entity does not have a process(es) to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing configuration. (Requirement R1 Part 1.2.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing configuration but did not verify and document that the required controls were not adversely affected following the change. (Requirement R1 Part 1.2.2 & Part 1.2.3) OR The Responsible Entity does not have a process for testing changes prior to implementing a change

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				tothe configuration. (Requirement R1 Part 1.3.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (Requirement R1 Part 1.3.2) OR The Responsible Entity does not have a process as specified in Part 1.4 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.4)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the items described in Requirement R1, Part 1.1. at least once every 35 calendar days. (Requirement R2 Part 2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for applicable systems, but has performed	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for applicable systems, but has performed	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for applicable systems, but has performed	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable systems. (Requirement R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable systems. (Requirement R3 Part 3.1)

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable systems. (Requirement R3 Part 3.2)	an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable systems. (Requirement R3 Part 3.2)	an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable systems. (Requirement R3 Part 3.2)	OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for applicable systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable systems.(Requirement R3 Part 3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable systems, but did not perform the active vulnerability assessment of its applicable systems. (Requirement R3 Part 3.3) OR The Responsible Entity has implemented one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				documented vulnerability assessment processes for each of its applicable systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Requirement R3 Part 3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-5, Requirement R4, Attachment 1, Section 1.1. (Requirement R4 Part R4) OR	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-5, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-5, Requirement R4, Attachment 1, Section 1.2. (Requirement R4) OR	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-5, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-5, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Section 1.2. (Requirement R4)	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.”.
- CIP-010-5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/18	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	
5	TBD	Virtualization modifications	

CIP-010-5 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting to a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of proposed standard for formal 10-day comment period.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security —~~ Configuration~~ Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5~~4~~

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5~~4~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic~~

~~Security Perimeters~~logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

~~4.2.3.2.~~4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

~~5.~~ **Effective Date:** See "Project 2016-02 Virtualization Implementation Plan." ~~for Project 2019-03.~~

~~**Background:** Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident~~

~~response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**"Applicable Systems" Columns in Tables:**~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented change management process(es) that collectively include each of the applicable requirement parts in *CIP-010-5~~4~~ Table R1 – ~~Configuration~~ Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5~~4~~ Table R1 – ~~Configuration~~ Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5~~4~~ Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	Authorize changes to~~Develop a baseline configuration, individually or by group, which shall include the following items~~: 1.1.1. Operating system(s) ~~(including version)~~ or firmware ~~where no independent operating system exists~~or images used to derive operating systems or firmware; 1.1.2. ~~Any c~~Commercially available or open-source application software ~~(including version) intentionally installed~~including Self-Contained Applications; 1.1.3. ~~Any c~~Custom software installed including Self-Contained Applications; 1.1.4. Any logical network accessible ~~ports~~services, (or logical ports if unable to determine service);	Examples of evidence may include, but are not limited to: - A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change. ~~A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or~~ ~~A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.~~

CIP-010-5~~4~~ Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	~~and~~ 1.1.5. ~~Any s~~Security patches applied;~~.~~ 1.1.6. SCI configuration that: - Enforces electronic access control that permits only needed and controlled communication between systems with different impact ratings hosted on SCI; - -Enforces logical isolation between systems with different impact ratings hosted on SCI; - Prevents sharing of CPU/Memory between systems with different impact ratings hosted on SCI; or - Enables or disables SCI services.	
~~1.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~	~~Authorize and document changes that deviate from the existing baseline configuration.~~	~~Examples of evidence may include, but are not limited to:~~ - ~~A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each~~

CIP-010-54 Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~2. PACS; and~~ ~~3. PCA~~		~~change; or~~ ~~• Documentation that the change was performed in accordance with the requirement.~~
~~**1.3**~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.~~	~~An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.~~
1.24	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	For ~~a~~ each change ~~that deviates from the existing baseline configuration~~to the items listed in Part 1.1: 1.2.1. Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.2.2. Following the change, verify that required cyber security controls determined in 1.24.1 are not	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-5~~4~~ Table R1 – ~~Configuration~~ Change Management

Part	Applicable Systems	Requirements	Measures
	SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	adversely affected; and 1.2.3. Document the results of the verification.	
1.3~~5~~	High Impact BCS SCI hosting High Impact BCS	~~Where technically feasible, f~~For each change ~~that deviates from the existing baseline configuration~~to the items listed in Part 1.1, per system capability: 1.3.1. Prior to implementing any change in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment ~~-~~or test the	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-5~~4~~ Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.3.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.~~6~~4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS	Prior to a change ~~that deviates from the existing baseline configuration~~ associated with ~~baseline items in~~Requirement Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.4~~6~~.1. Verify the identity of the software source; and 1.4~~6~~.2. Verify the integrity of the software obtained from the	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-54 Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI hosting High or Medium Impact BCS and their associated EACMS and PACS. Management Modules of SCI hosting High or Medium Impact BCS and their associated EACMS and PACS. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.4~~6~~: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	software source.	

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~4~~ 5 Table R2 – ~~Configuration~~ Change Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~4~~ 5 Table R2 – ~~Configuration~~ Change Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-54 Table R2 – ~~Configuration~~ Change Monitoring

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for unauthorized changes to the ~~baseline configuration (as~~items described in Requirement R1, Part 1.1~~)~~. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~3~~ 5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~ 5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~4~~5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: - PACS; - EACMS; or - PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: - A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or - A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~4~~ 5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems SCI hosting High Impact BCS. Management Modules of SCI hosting High Impact BCS.	~~Where technically feasible, a~~At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects~~, that models the baseline configuration of the BES Cyber System in a production environment~~; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~4~~ 5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BES Cyber Systems or their associated: - PACS; - EACMS; or - PCA Management Modules of SCI hosting High Impact BCS or their associated: - EACMS; or - PCA	Perform an active vulnerability assessment prior to logically connecting an additional applicable Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure to a production environment, per system capability~~Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset~~, except for CIP Exceptional Circumstances, or ~~and like replacements~~deployments ~~of the same type of Cyber Asset with~~using a ~~baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset~~previously assessed configuration. The production environment does not include devices being actively remediated and logically isolated.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure) and the output of any tools or Management Systems used to perform the assessment.

3.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PACS; • EACMS; or • PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a report of Management System actions, or a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated SCI and Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.	The Responsible Entity has documented and implemented a ~~configuration~~ change management process(es) that includes only four or more of the required ~~baseline~~ items listed in 1.1.1 through 1.1.6~~5~~. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a ~~configuration~~ change management process(es) that includes only three of the required ~~baseline~~ items listed in 1.1.1 through 1.1.6~~5~~. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a ~~configuration~~ change management process(es) that includes only two of the required ~~baseline~~ items listed in 1.1.1 through 1.1.6~~5~~. (Requirement R1 Part 1.1) OR The Responsible Entity has a process as specified in Part 1.~~6~~4 to verify the identity of the software source (1.~~6~~4.1) but does not have a process as specified in Part 1.~~6~~ 4 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.~~6~~4.2)	The Responsible Entity has not documented or implemented any ~~configuration~~ change management process(es). (Requirement R1) OR The Responsible Entity has documented and implemented a ~~configuration~~ change management process(es) that includes only one of the required ~~baseline~~ items listed in 1.1.1 through 1.1.6~~5~~. (Requirement R1 Part 1.1) OR The Responsible Entity does not have a change management process(es) that requires authorization ~~and documentation~~ of changes ~~that deviate from the existing baseline~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~configuration~~to items listed in 1.1.1-1.1.6. (Requirement R1 Part 1.1~~2~~) ~~OR~~ ~~The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3)~~ OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing ~~baseline~~ configuration. (Requirement R1 Part 1.~~4~~2.1) OR The Responsible Entity has a process(es) to determine required security controls in

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing ~~baseline~~ configuration but did not verify and document that the required controls were not adversely affected following the change. (Requirement R1 Part 1.~~4~~2.2 & Part 1.~~4~~2.3) OR The Responsible Entity does not have a process for testing changes~~ in an environment that models the baseline configuration~~ prior to implementing a change ~~that deviates from baseline~~to the configuration. (Requirement R1 Part 1.~~5~~3.1) OR The Responsible Entity does not have a process to document the test results and, if using a test

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				environment, document the differences between the test and production environments. (Requirement R1 Part 1.~~5~~3.2) OR The Responsible Entity does not have a process as specified in Part 1.~~6~~4 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.~~6~~4)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the items described in Requirement R1, Part 1.1.

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				~~the baseline~~ at least once every 35 calendar days. (Requirement R2 Part 2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for ~~A~~applicable s~~S~~ystems, but has performed an active vulnerability assessment more than 36 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for a~~A~~pplicable s~~S~~ystems, but has performed an active vulnerability assessment more than 39 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for a~~A~~pplicable s~~S~~ystems, but has performed an active vulnerability assessment more than 42 months, but	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable ~~BES Cyber S~~systems. (Requirement R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	less than 39 months, since the last active assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.2)	less than 42 months, since the last active assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.2)	less than 45 months, since the last active assessment on one of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.2)	documented active vulnerability assessment processes for a~~A~~pplicable s~~S~~ystems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable ~~BES Cyber S~~systems.(Requirement R3 Part 3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but did not perform the active vulnerability assessment ~~in a manner that models an existing baseline configuration~~ of its applicable ~~BES Cyber S~~systems. (Requirement R3 Part 3.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable ~~BES Cyber S~~systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Requirement R3 Part 3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-45, Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-45, Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-45, Requirement R4,	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-45, Requirement R4. (R4)

R #	**Violation Severity Levels**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	Attachment 1, Section 1.1. (Requirement R4 Part R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-45, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Section 1.2. (Requirement R4)	Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document	Attachment 1, Section 1.2. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-45, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.” ~~for Project 2019-03~~.
- CIP-010-~~4~~ 5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	
5	TBD	Virtualization modifications	

CIP-010-5~~4~~ - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber

Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting to a ~~using a Cyber Asset other than a~~ BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-~~4~~ 5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-3

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. Generator Operator

    4.1.4. Generator Owner

    4.1.5. Reliability Coordinator

    4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-011-3:

4.2.3.1. Cyber systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

6. **Effective Dates:** See “Project 2016-02 Virtualization Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems (BCS) and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI hosting High or Medium Impact BCS or their associated: • EACMS; or • PACS.	Method(s) to identify information that meets the definition of BCSI.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BCSI from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BCSI; or • Repository or electronic and physical location designated for housing BCSI in the entity's information protection program.

CIP-011-3 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS and their associated: 1. EACMS; and 2. PACS SCI hosting High or Medium Impact BCS or their associated: • EACMS; or • PACS	Procedure(s) for protecting and securely handling BCSI, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3 Table R2 –Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-3 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3 Table R2 –Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: • EACMS; • PACS; or • PCA	Method(s) to prevent the unauthorized retrieval of BCSI from applicable systems prior to their disposal or reuse (except for reuse within other systems identified in the "Applicable Systems" column).	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. **Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program**

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-011-3)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a BCSI protection program (Requirement R1).
R2.	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (Requirement R2 Part 2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (Requirement R2 Part 2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal. (Requirement R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-3~~2~~

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1. Balancing Authority

      4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

            4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

      4.1.3. Generator Operator

      4.1.4. Generator Owner

~~4.1.5. Interchange Coordinator or Interchange Authority~~

~~4.1.6.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-011-3~~2~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic~~

~~Security Perimeters~~logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.

~~4.2.3.2.~~4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

5. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

5. **Effective Dates:** See "Project 2016-02 Virtualization Implementation Plan." ~~for CIP-011-3~~~~2.~~

~~6. **Background:** Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and~~

~~Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

~~**High Impact BES Cyber Systems –**~~ ~~Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems –**~~ ~~Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Electronic Access Control or Monitoring Systems (EACMS) –**~~ ~~Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS) –**~~ ~~Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

~~**Protected Cyber Assets (PCA) –**~~ ~~Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-3~~2~~ Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-3~~2~~ Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3~~2~~ Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems (BCS) and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI hosting High or Medium Impact BCS or their associated: - EACMS; or - PACS.	Method(s) to identify information that meets the definition of ~~BES Cyber System Information~~BCSI.	Examples of acceptable evidence include, but are not limited to: - Documented method to identify ~~BES Cyber System Information~~BCSI from entity's information protection program; or - Indications on information (e.g., labels or classification) that identify ~~BES Cyber System Information~~BCSI as designated in the entity's information protection program; or - Training materials that provide personnel with sufficient knowledge to recognize ~~BES Cyber System Information~~BCSI; or - Repository or electronic and physical location designated for housing ~~BES Cyber System Information~~BCSI in the entity's information protection program.

CIP-011-3~~2~~ Table R1 – Information Protection

Part	Applicable Systems	Requirements	Measures
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS SCI hosting High or Medium Impact BCS or their associated: • EACMS; or • PACS	Procedure(s) for protecting and securely handling ~~BES Cyber System Information~~BCSI, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of ~~BES Cyber System Information~~BCSI; or • Records indicating that ~~BES Cyber System Information~~BCSI is handled in a manner consistent with the entity’s documented procedure(s).

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-3~~2~~ Table R2 –*~~*BES Cyber Asset*~~ *Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-3~~2~~ Table R2 –*~~*BES Cyber Asset*~~ *Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-3~~2~~ Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated: - EACMS; - PACS; or - PCA	Method(s) ~~Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action~~ to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from applicable systems prior to~~upon~~ their disposal or reuse (except for reuse within other systems identified in the “Applicable Systems” column). ~~outside another applicable systemthe Cyber Asset data storage media.~~	Examples of acceptable evidence include, but are not limited to: - Records tracking sanitization actions taken to prevent unauthorized retrieval of ~~BES Cyber System Information~~BCSI such as clearing, purging, or destroying; or - Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of ~~BES Cyber System Information~~BCSI.

CIP-011-3~~2~~ Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~2.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.~~	~~Examples of acceptable evidence include, but are not limited to:~~ ~~• Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or~~ ~~• Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.~~

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~**1.3. Compliance Monitoring and Assessment Processes:**~~

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Violation Investigations~~
- ~~Self-Reporting~~
- ~~Complaints~~

~~**1.4. Additional Compliance Information:**~~

~~None.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-011~~0~~-3~~2~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a ~~BES Cyber System Information~~BCSI protection program (Requirement R1).
R2.	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from the BES Cyber Asset. (Requirement R2 Part 2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of ~~BES Cyber System Information~~BCSI from the BES Cyber Asset. (Requirement R2 Part 2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-3~~2~~ Table R2 – BES Cyber Asset Reuse and Disposal. (Requirement R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See "Project 2016-02 Virtualization Implementation Plan. ~~Guideline and Technical Basis (attached).~~

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	TBD	Virtualization conforming changes	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.~~

~~The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.~~

~~The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.~~

~~Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.~~

~~The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.~~

~~A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.~~

~~Requirement R2:~~

~~This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.~~

~~The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.~~

~~If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.~~

~~Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.~~

~~The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:~~

> ~~Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].~~
>
> ~~Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for~~

~~quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.~~

~~Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.~~

~~In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.~~

~~It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization~~ processes.

~~Rationale~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.~~

~~Rationale for Requirement R2:~~

~~The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**
2. **Number:** **CIP-013-3**
3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems and their associated cyber systems.
4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider:** One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers:** All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-013-3:

4.2.3.1. Cyber systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems (BCS) or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See “Project 2016-02 Virtualization Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems, their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and the SCI hosting high or medium impact BCS or their associated Electronic Access Controlling or Monitoring System (EACMS) or Physical Access Control System (PACS). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of SCI, BCS, and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System (BES) from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring SCI, BCS, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the SCI, BCS and their associated EACMS and PACS; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the

scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do not include one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do not include two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				cyber security risk management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2; OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	R1 Part 1.2.1 through Part 1.2.6.	Requirement R1 Part 1.2.1 through Part 1.2.6.		The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan”

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	
3	TBD	Virtualization conforming changes.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
45-day formal comment period with ballot	January 21–February 8, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3~~2~~**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems and their associated cyber systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-3~~2~~:

4.2.3.1. Cyber ~~Assets~~ systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ systems associated with communication ~~networks and data communication~~ links ~~between discrete Electronic Security Perimeters (ESPs)~~logically isolated from, but not providing logical isolation for, BES Cyber Systems (BCS) or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See “Project 2016-02 Virtualization Implementation Plan.” ~~for Project 2019-03.~~

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact ~~-~~BES Cyber Systems, ~~and~~ their associated Electronic Access Control or Monitoring Systems (EACMS), ~~and~~ Physical Access Control Systems (PACS), and the SCI hosting high or medium impact BCS or their associated Electronic Access Controlling or Monitoring System (EACMS) or Physical Access Control System (PACS). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of SCI, ~~BES Cyber Systems~~BCS, and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System (BES) from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring SCI, ~~BES Cyber Systems~~BCS, and their associated EACMS and PACS, that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the SCI, ~~BES Cyber System~~BCS and their associated EACMS and PACS; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the

scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do not include one of the parts	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do not include two or more of the parts in Requirement R1	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	in Requirement R1 Part 1.2.1 through Part 1.2.6.	Part 1.2.1 through Part 1.2.6.		OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring ~~BES Cyber~~	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring ~~BES Cyber~~	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~BES Cyber Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.	~~BES Cyber Systems and their associated EACMS and PACS~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan” f~~or Projec~~t ~~2019-03~~
- ~~CIP-013-2 Technical Rationale~~

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	
3	TBD	Virtualization conforming changes.	

Project 2016-02 Virtualization Implementation Plan

Applicable Standard(s)

- Reliability Standard CIP-002-7 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-9 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-7 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-8 – Cyber Security – BES Cyber System Logical Isolation
- Reliability Standard CIP-006-7 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-7 – Cyber Security – System Security Management
- Reliability Standard CIP-008-7 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-5 – Cyber Security – Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-3 – Cyber Security – Information Protection
- Reliability Standard CIP-013-3 – Cyber Security – Supply Chain Risk Management
- Proposed new or modified terms listed in the “CIP Definitions Posting Document (Project 2016-02)”

  These standards and Definitions of Terms used in the versions listed above of the CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

  These standards and new and modified terms used in the standards above will be referenced as the “Revised CIP Standards and Definitions” within the Implementation Plan.

Requested Retirement(s)

- Reliability Standard CIP-002-6 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-8 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-6 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)
- Reliability Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-6 – Cyber Security – System Security Management
- Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning

- Reliability Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-2 – Cyber Security – Information Protection
- Reliability Standard CIP-012-1 – Cyber Security – Communications between Control Centers
- Reliability Standard CIP-013-2 – Cyber Security – Supply Chain Risk Management
- Proposed terms for retirement listed in the "Definitions of Terms used in the above listed CIP Cyber Security Standards" document

These standards and definitions used in the versions listed above will be referenced as the "Requested CIP Retired Standards and Definitions" within the Implementation Plan.

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved or retired before the Applicable Standard become effective:

- BES Cyber Asset (BCA)
- BES Cyber System
- BES Cyber System Information
- CIP Senior Manager
- Cyber Asset
- Cyber Security Incident
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate Systems (IS)
- Management Interface
- Management Module
- Management Systems
- Physical Access Control Systems
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Removable Media
- Reportable Cyber Security Incident
- Self-Contained Application
- Shared Cyber Infrastructure (SCI)
- Transient Cyber Asset (TCA)
- Virtual Cyber Asset (VCA)

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions. The intent of the Compliance Dates for Early Adoption of Revised CIP Standards and Definitions section is to permit Responsible Entities the adoption to comply with the Revised CIP Standards and Definitions prior to the Effective Date.

Effective Date and Phased-in Compliance Dates

The Effective Dates for the Revised CIP Standards and Definitions are provided below. As noted in the General Considerations section above, the standard drafting team determined to clarify initial performance of periodic requirements and permit Responsible Entities to comply with the Revised CIP Standards and Definitions prior to the effective date. These provisions also are provided below.

Revised CIP Standards and Definitions

Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the date the Revised CIP Standards and Definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

---

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards and Definitions.

Compliance Dates for Early Adoption of Revised CIP Standards and Definitions

A Responsible Entity may elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the Revised CIP Standards and Definitions. Responsible Entities must comply with applicable Requested CIP Retired Standards and Definitions until that date.

Retirement Date

Requested CIP Retired Standards and Definitions

The Requested CIP Retired Standards and Definitions shall be retired immediately prior to the effective date of the Revised CIP Standards and Definitions in the particular jurisdiction in which the Revised CIP Standards and Definitions are becoming effective.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards

Do not use this form for submitting comments. Use the [Standards Balloting and Commenting System (SBS)]() to submit comments on the **Virtualization Modifications** by **8 p.m. Eastern, Monday, March 22, 2021.**

Additional information is available on the [project page](). If you have questions, contact Senior Standards Developer, [Jordan Mallory]() (via email) or at 404-446-2589.

Background Information

Project 2016-02 (1) addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and (2) considers the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for standard drafting team (SDT) consideration (V5TAG Transfer Document).

The V5TAG, which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP Version 5 standards and to support industry's implementation activities. During the V5TAG's activities, it identified certain issues with the CIP Reliability Standards that would be better addressed by a SDT for the CIP Reliability Standards. The V5TAG developed the [CIP Version 5 Transition Advisory Group Issues for Consideration]() document to formally recommend that the SDT address these issues and consider modifications to the standard language during the standards development process. Among other issues, the V5TAG stated "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

SDT Approach

As the SDT investigated these issues, it found that virtualization affects most of the technical definitions used within the CIP Standards from the foundational "Cyber Asset" to the technical CIP standards (CIP-005, CIP-007, and CIP-010 in particular). This is due to virtualization changing fundamental assumptions, such as the standards having an "electronic device" basis, focusing on routable protocol level only, and perimeter-based security. The SDT found virtualization to be not only a driver of change, but a symptom of a larger issue with the standard's ability to adapt to current and future technology innovation. The SDT concluded these more technical standards could benefit from removing inherent prescription of certain architectures and moving requirements to an objective or results-oriented level that do not make assumptions about architecture. In other words, the standards should not go further and prescribe how to secure today's newer architectures but should require that certain security objectives be met and "get out of the way" of virtualization and future innovations that can increase reliability, resiliency, and security of our BES Cyber Systems.

The SDT has been addressing these issues and has gathered feedback from stakeholders through conceptual webinars and technical conferences. The SDT has progressed from a general direction of "cyber system orientation and objective-level requirements" to now having the concepts drafted into proposed technical standards (CIP-005, CIP-007, and CIP-010) and conforming virtualization revisions to the remaining CIP standards that are not directly affected by virtualization or technology changes.

As part of the Standard Authorization Request (SAR) for this project, the SDT also reviewed the addition of CIP Exceptional Circumstances (CEC) to new and existing requirements. The SDT determined that CEC could be applied to the following additional requirements, CIP-004-7 R2.2, CIP-004-7 R3.5, CIP-006-7 R1.8, CIP-006-7 R1.9, CIP-006-7 R2, CIP-010-5 R1.2, and CIP-010-5 R1.3.

Additionally, the SDT modified CIP-002 Attachment 1, Criterion 2.1 to align with a previously approved response to a Request for Interpretation (RFI) regarding "shared BES Cyber Systems." The SDT's response to the RFI was originally included in Appendix 1 of CIP-002-5.1a. CIP-002, Attachment 1 Criterion 2.1 was modified to align with the previously approved RFI response. The proposed revision to Criterion 2.1 now states that the only BES Cyber Systems that meet criterion 2.1 are each discrete shared BES Cyber System that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Summary of Proposed Definition Changes

The following provides rationale and updates the associated definitions.

Term to be Retired	Rationale for Retirement
Electronic Access Point (EAP)	With the proposed revisions of CIP-005-6 Requirement R1 Part 1.2 this definition is no longer required. The isolation concepts in proposed Requirement R1 Parts 1.1, 1.2, and 1.3 address the necessary controls previously defined in the concept of an identified Electronic Access Point.
Electronic Security Perimeter (ESP)	This term is proposed for retirement. Isolation concepts are now described in Requirement R1 Parts 1.1, 1.2, and 1.3, to enable virtualization and future technologies. The SDT modified the requirement parts to remove the direct reference to a perimeter model.

The CIP SDT Proposed new or revised definitions to incorporate virtualization and future technology. The **bullet points below provide rationale** for a number of the definitions. Please see the CIP Definitions document for all new and revised definitions.

- **BES Cyber Asset (BCA)** – This SDT proposes to retain the BCA definition with updates to include the proposed term "Virtual Cyber Asset (VCA)." A BCA consists of a Cyber Asset or VCA that meets the qualifying language of a BCA (15 min impact, etc.).
- **BES Cyber System (BCS)** – The SDT proposes to retain the definition for BCS, with the addition of the acronym "BCS" in the Glossary of Terms used in NERC Reliability Standards (Glossary).

- **BES Cyber System Information (BCSI)** – This term was updated to add Shared Cyber Infrastructure to the scope of information covered within the BCSI definition. The SDT also proposes adding the acronym "BCSI" within the Glossary.
- **CIP Senior Manager** – This term was updated to remove the reference "CIP-002 through CIP-011" from the definition.
- **Cyber Asset** – This term was modified to ensure that Shared Cyber Infrastructure (SCI) is excluded from the Cyber Asset definition. SCI is a proposed term and is identified as a distinct applicable system throughout the CIP Standards.
- **Electronic Access Control or Monitoring Systems (EACMS)** - The SDT proposes revising this term to include applicable VCA and SCI within the definition of EACMS. The proposed revisions replace the retired term Electronic Security Perimeter (ESP) with logical isolation to transition from prescriptive technologies and conform with proposed revisions in CIP-005-8.
- **External Routable Connectivity (ERC)** – This term has been revised to include SCI and VCA. The SDT also removed the reference to ESP and added scoping language within the definition.
- **Interactive Remote Access (IRA)** – The SDT removed the reference to an ESP and added scoping language to scope remote access.
- **Intermediate Systems (IS)** – This term was revised to identify IS as EACMS that are used to restrict Interactive Remote Access (IRA). References to an ESP were removed from the definition.
- **Management Interface** – The SDT proposes adding this new term to the Glossary. A Management Interface is a physical or logical interface of a Cyber Asset or SCI that provides management and monitoring capabilities. This term is referenced as an applicable system throughout the revised standards.
- **Management Module** – The SDT proposes adding this term to the Glossary to identify autonomous subsystems of Cyber Assets or SCI that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system. This term is referenced as an applicable system throughout the revised standards.
- **Management Systems** - The SDT proposes adding this term to the Glossary to define any combination of Cyber Asset or VCA that establish and maintain the integrity of VCA or Cyber Asset through control of the processes for initializing, deploying, and configuring those assets and systems. This definition excludes Management Modules.
- **Physical Access Control Systems** – This term was retained and updated to include SCI.
- **Protected Cyber Asset (PCA)** – This term was retained and updated to specifically exclude SCI.
- **Removable Media** – This term was retained and updated with references to the new term SCI.
- **Reportable Cyber Security Incident** – The SDT revised this term to transition from ESP to logical isolation. The definition was also updated to include compromises or disruptions to SCI of a high or medium impact BCS.
- **Self-Contained Application** – The SDT proposes adding this definition to the Glossary to identify Self-Contained Applications as applicable systems throughout the CIP Standards. Self-Contained

Applications are immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment.

- **Shared Cyber Infrastructure (SCI)** – The SDT proposes adding this definition to the Glossary to identify electronic devices and their software that share their compute or storage resources with one or more BES Cyber Systems, or their associated EACMS, Physical Access Control Systems (PACS), and Protected Cyber Asset (PCA). The SDT proposes identifying SCI within CIP-002-7 and it is an applicable system throughout the proposed CIP Standards.
- **Transient Cyber Asset (TCA)** – The SDT retained this definition and updated it to include the proposed term VCA. The proposed definition excludes SCI associated with high or medium impact BCS.
- **Virtual Cyber Asset (VCA)** – The SDT proposes adding this definition to the Glossary to identify the logical instance of an operating system or firmware hosted on SCI or a Cyber Asset.

Summary of CIP-005 Changes

For a detailed explanation of these changes, please refer to the *CIP-005 Technical Rationale* document.

CIP-005 has been modified to accommodate three major areas:

1) Allow for network security models that are not perimeter-based, such as zero trust models. Perimeter-based models (such as ESP) remain a valid option, but are no longer the prescribed option.
2) Requiring the protection and isolation of the management plane of SCI.
3) Allow for single ESPs or logical isolation methods to span geographic locations by requiring the protection of the data, while keeping the Cyber Assets between the sites out of scope (e.g. carrier's telecom equipment).

Summary of CIP-007 Changes

For a detailed explanation of these changes, please refer to the *CIP-007 Technical Rationale* document. CIP-007 changes consist primarily of conforming changes that add the new virtualization types including SCI to the scope of applicable systems. It also changes the focus of "ports and services" to the services while still allowing port number's to be tracked. Port numbers are merely pointers to a service such as SSH, web server, database server, DNP or Modbus server or client, etc. In virtualized environments, the focus moves more to what services are enabled and port numbers take on a lesser role. The language has been modified to reflect this.

Summary of CIP-010 Changes

For a detailed explanation of these changes, please refer to the *CIP-010 Technical Rationale* document. The proposed changes in CIP-010-5 concern the use of several facets of virtualization technologies. Virtualization allows for such technologies as new logical isolation controls for SCI, remediation VLANs, parent/child images, dormant virtual machines (VMs), and self-contained applications (containers). Enabling and clarifying the use of these technologies is the basis of the proposed changes in CIP-010-5. CIP-010 Requirement R1 also changes focus from maintaining baseline configurations to authorizing change to an expanded list of configuration attributes that are used to secure virtualized environments.

Summary of Conforming Changes

For a detailed explanation of these changes, please refer to the *Technical Rationale* document for CIP-002, CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013. The conforming changes to all standards are primarily to add the new term SCI to the scope of requirements throughout the standards. The SDT also replaced TFE's with the "per system capability" language, updated the Exemption Section in each standard to conform to the CIP-005 changes above. Also, any prescriptive references to ESP's have been removed per the CIP-005 discussion above.

Questions

1. The SDT added, revised, and retired several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

2. CIP-005 Requirement R1 part 1.1 was revised to permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

3. The SDT modified CIP-005 Requirement R1 Part R1.2 to establish logical isolation requirements for Management Systems, Management Interfaces, and associated SCI. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No
   Comments:

4. The SDT modified CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters. Does the proposed requirement fulfill the directive from FERC Order 791, paragraph 150? Please provide the basis for your response.

   ☐ Yes
   ☐ No

   Comments:

5. The SDT modified CIP-005 Requirement R2 to ensure remote access management requirements align with the new and revised virtualization terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

6. The SDT revised CIP-007 Requirement R1 Part 1.1 to shift the security objective from logical network accessible ports to services. The proposed revisions require Responsible Entities to enable only network accessible services that have been determined to be needed by the Responsible Entity. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

7. CIP-010 Requirement R1 currently requires Responsible Entities to develop a baseline configuration, authorize changes to the baseline, and document the changes. The SDT proposes to revise Requirement R1 to remove the reference to baseline configurations. The proposed revisions require the authorization of changes to Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible ports, security patches applied, and SCI configurations. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

8. The SDT modified CIP-010 Requirement R3 Part 3.3 to ensure that vulnerability assessments are performed prior to logically connecting Cyber Assets, VCA, and SCI. The revised requirement allows the use of remediation VLANs to perform active vulnerability assessments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

9. CIP-002-5.1a includes exemption 4.2.3.2, which exempted Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. In the development of conforming changes, the SDT determined that the exemption should be split into two distinct exemptions to adequately cover all cyber systems associated with conforming changes. The SDT established those conforming changes in proposed Exemptions 4.2.3.2 & 4.2.3.3. Do the changes clearly identify the exempted cyber systems? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

10. BCS and SCI are mutually exclusive by definition, however SCI poses a significant reliability risk to the Bulk Electric System. The SDT considered the risks associated with SCI and revised CIP-002 Requirement R1 to include the identification of SCI in Parts 1.3, 1.4, and 1.5. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

    ☐ Yes
    ☐ No

    Comments:

11. In the current enforceable standards, there are no requirements that can be used to tie a non-identification of EACMS, PACS, and PCAs to a single requirement. The SDT revised CIP-002 to include the identification of SCI associated with EACMS, PACS, and PCAs to help address this issue within the virtualization scope of the current SAR. The proposed requirement could reduce possible non-compliance to a single issue if a Responsible Entity fails to properly identify SCI associated with EACMS, PACS, or PCAs. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

    ☐ Yes
    ☐ No

    Comments:

12. The SDT modified CIP-002 Attachment 1, Criterion 2.1 to align with a previously approved Request for Interpretation (RFI) regarding “shared BES Cyber Systems.” The SDT modified the criterion to reference each discrete shared BCS. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

    ☐ Yes
    ☐ No

    Comments:

13. The SDT made conforming changes to CIP-003 and CIP-004. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

    ☐ Yes
    ☐ No

    Comments:

14. The SDT modified the Applicable Systems column in CIP-006 to include SCI hosting PACs associated with Medium Impact BCS with ERC or IRA. The SDT made the proposed revisions to clarify the scope of requirements that apply when an entity implements serial IRA. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

15. The SDT made conforming changes to CIP-008 and CIP-009. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

16. The SDT modified CIP-011 Requirement R2 part 2.1, which will allow cryptographic erasure in scenarios where BCSI can't be mapped to particular disks in virtualized storage. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

17. The SDT performed a review of the CIP Standards and determined that CIP Exceptional Circumstances could be applied to the following additional requirements: CIP-004-7 Requirement R2 Part 2.2, CIP-004-7 Requirement R3 Part 3.5, CIP-006-7 Requirement R1 Part 1.8, CIP-006-7 Requirement R1 Part 1.9, CIP-006-7 Requirement R2, CIP-010-5 Requirement Part 1.2, and CIP-010-5 Requirement R1 Part 1.3. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

18. Implementation Plan: The SDT proposes an Implementation Plan that makes the revised CIP Standards and definitions effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order. However, the implementation plan allows a Responsible Entity to elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. Do you agree with this proposal? If you think an alternate effective date is needed, please provide a detailed explanation of actions and time needed.

   ☐ Yes
   ☐ No

   Comments:

19. Please provide any additional comments for the SAR drafting team to consider, if desired.

CIP Definitions

Project 2016-02 Modifications to CIP Standards

This standards drafting team (SDT) is seeking comment on the following new, modified, or retired terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new glossary term. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in the redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS)	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
BES Cyber System Information (BCSI)	Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	Information about the BES Cyber System or Shared Cyber Infrastructure that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context~~, ESP names~~, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Standards~~, CIP-002 through CIP-011.~~
Cyber Asset	Programmable electronic devices, including the hardware, software, and data in those devices.	Programmable electronic devices, including the hardware, software, and data in those devices; excluding Shared Cyber Infrastructure.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: ~~•~~ For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) ~~an~~ • ~~Electronic Security Perimeter~~the logical isolation, (2) a Physical Security Perimeter,~~ or~~ (3) an Electronic Access Control or Monitoring System, or (4) Shared Cyber Infrastructure; or • Disrupts or attempts to disrupt the operation of a BES Cyber System
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of the logical isolation ~~Electronic Security Perimeter(s)~~ of~~r~~ BES Cyber Systems. This includes Intermediate Systems.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	Proposal to retire.
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset or Virtual Cyber Asset through an Electronic Access Control or Monitoring System controlling communications to and from the BES Cyber System ~~that is outside of its associated Electronic Security Perimeter~~ via a bi-directional routable protocol connection.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	Proposal to retire.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated access by a person employing a remote access client from outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed. ~~or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.~~
Intermediate Systems	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	An Electronic Access Control or Monitoring System that is used to restrict Interactive Remote Access.~~A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.~~
Management Interface **New Definition**		A physical or logical interface of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Management Module **New Definition**		An autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.
Management Systems **New Definition**		Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Cyber Assets or Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers	Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	One or more Cyber Assets or Virtual Cyber Assets that: • Are not logically isolated from a BES Cyber System; or • Share CPU or memory with a BES Cyber System; excluding Shared Cyber Infrastructure, excluding logically isolated Cyber Assets or Virtual Cyber Assets that are being actively remediated prior to introduction to the production environment. ~~connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.~~
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, Shared Cyber Infrastructure, or a ~~network within an ESP, or a~~ network that is not logically isolated from high or medium impact BES Cyber Systems. ~~Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	A Cyber Security Incident that compromised or disrupted: • ~~–~~A BES Cyber System that performs one or more reliability tasks of a functional entity; • ~~- An Electronic Security Perimetert~~The logical isolation of a high or medium impact BES Cyber System; ~~or~~ • ~~–~~An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or • - Shared Cyber Infrastructure of a high or medium impact BES Cyber System
Self-Contained Application **New Definition**		Immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment.
Shared Cyber Infrastructure (SCI) **New Definition**		One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	A Cyber Asset or Virtual Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, ~~2.~~3. not a Shared Cyber Infrastructure associated with high or medium impact BES Cyber Systems, ~~3.~~4. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and ~~4.~~5. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • Shared Cyber Infrastructure, • Network ~~within an Electronic Security Perimeter containingt~~ that is not logically isolated from high or medium impact BES Cyber Systems, or • Protected Cyber Asset associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Virtual Cyber Asset (VCA) **New Definition**		A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure or a Cyber Asset.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2016-02 Modification to CIP Standards

Definitions and Exemptions Technical Rationale

Proposed Modified Terms

BES Cyber Asset (BCA)

A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Rationale

The BCA definition is changing to allow for BCA to be either Cyber Assets (hardware included) or Virtual Cyber Assets (VCA) (software only virtual machines without the underlying hardware). The definition of BCA excludes the underlying hardware for virtualized environments, now defined as Shared Cyber Infrastructure (SCI). The standards drafting team (SDT) recognizes that SCI indeed has the same impact as a virtual BCA and even more so if hosting numerous BCA, and those risks will be addressed in requirements specifically for the SCI. See the VCA and SCI definition below.

BES Cyber System (BCS)

No proposed change to definition, only addition of BCS acronym to the NERC Glossary.

Rationale

In order to shorten several applicability statements within the body of CIP standards, the SDT proposes that “BCS” be added as the defined acronym for “BES Cyber System” to the NERC glossary.

BES Cyber System Information (BCSI)

Information about the BES Cyber System or Shared Cyber Infrastructure that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System

Rationale

Conforming changes such that BCSI includes information about SCI.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Standards.

Rationale

Remove explicit reference to the CIP standards as only "CIP-002 through CIP-011" as the body of CIP standards has grown beyond CIP-011. As an example, the CIP Senior Manager also has requirements within CIP-013.

Cyber Asset

Programmable electronic devices, including the hardware, software, and data in those devices; excluding Shared Cyber Infrastructure.

Rationale

Modified to explicitly exclude SCI from the definition of CA such that SCI and CA are two hardware 'forms' on which the other types of cyber systems reside. SCI is another form of 'programmable electronic device' that does NOT include the software and data in the hardware device. SCI is defined separately such that it can be the object of additional requirements based on its unique risks.

Cyber Security Incident

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) the logical isolation, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System, or (4) Shared Cyber Infrastructure; or
- Disrupts or attempts to disrupt the operation of a BES Cyber System

Rationale

Modified to refer to logical isolation instead of ESPs as well as add SCI to the scope of compromised or attempted compromise systems.

Electronic Access Control or Monitoring Systems (EACMS)

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of the logical isolation of BES Cyber Systems. This includes Intermediate Systems.

Rationale

Modified to add VCA and SCI as two other forms that an EACMS can take. Changed the reference to ESP to 'logical isolation'.

External Routable Connectivity (ERC)

The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset or Virtual Cyber Asset through an Electronic Access Control or Monitoring System controlling communications to and from the BES Cyber System via a bi-directional routable protocol connection.

Rationale

The ERC definition is used throughout the CIP Standards within the Applicable Systems column as a scoping mechanism based on the inherent risk associated with external routable connectivity. In order to maintain the correct ERC scoping the SDT made conforming changes only to the ERC definition. The definition was modified to include Virtual Cyber Assets as potential remote clients, added SCI as potential targets, and replaced the ESP as the only model with the more generic "through an EACMS controlling communications…" that allows non-perimeter-based models.

Interactive Remote Access (IRA)

User-initiated access by a person employing a remote access client from outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed.

Rationale

The IRA definition is changing to remove its dependency on ESP and remove several requirements and scoping mechanisms that were embedded within it resulting in a simpler definition. The requirements and scoping mechanisms have been moved into CIP-005 R2. The references to ownership of the remote client have been removed as immaterial to the CIP-005 requirements. The reliance on "using a routable protocol" has been removed to incorporate serial non-routable target Cyber Assets that are converted to routable protocols (serial to IP converters) and therefore have the same IRA capability as native routable protocol target Cyber Assets. This clarification was one of the issues from the V5TAG effort the SDT is to address. The "from outside of the asset containing the system being accessed" was added to clarify that local TCA connections even if using a 'remote access client' are not IRA. The "outside of the logical isolation" was used to allow for non-perimeter-based network models, replacing ESP as the only option.

Intermediate Systems (IS)

A type of Electronic Access Control or Monitoring System that is used to restrict Interactive Remote Access.

Rationale

The IS definition is changing to remove requirement language (e.g. where an IS must reside and how it must control IRA) that was embedded within the definition. Such language has been moved to CIP-005 R2 so that it is a mandatory requirement.

Physical Access Control Systems (PACS)

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Rationale

This definition is changing to allow Virtual Cyber Assets or SCI as a form that a PACS can take.

Physical Security Perimeter (PSP)

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Rationale

The PSP definition is changing to add SCI as type of device which must be within a PSP.

Protected Cyber Asset (PCA)

One or more Cyber Assets or Virtual Cyber Assets that:

- Are not logically isolated from a BES Cyber System; or
- Share CPU or memory with a BES Cyber System; excluding Shared Cyber Infrastructure,

excluding logically isolated Cyber Assets or Virtual Cyber Assets that are being actively remediated prior to introduction to the production environment.

Rationale

The PCA definition is being updated to remove the dependency on ESP and allow for other methods of logical isolation. It is also being updated to include “share compute resources (CPU or memory) with a BES Cyber System” to mitigate the risks of hardware-based vulnerabilities (Spectre, Meltdown, Rowhammer, etc.) on Shared Cyber Infrastructure for any virtual machines allowed to run on the same hardware as BES Cyber Systems. Since virtualization can allow systems of differing trust levels to simultaneously execute on the same hypervisor servers in the hardware underlay and thus share the same CPU and memory, this addition to the PCA definition requires that those VCAs that do share CPU and memory become associated PCA’s of any BES Cyber Systems sharing the same hypervisor compute resources. This provides the high water marking of VCAs sharing a single hypervisor’s CPU or memory. Affinity rules can be used within the environment to prevent this situation and keep other virtual machines from becoming PCAs. Finally, the definition is being modified to account for “remediation VLAN” automation of security controls where a VCA may instantiate in a logical network reserved for vulnerability assessment and updates (OS patches, AV updates, etc.). The intent is the VM does not become a PCA while in this state as its being updated prior to being connected to its production network.

Removable Media

Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, Shared Cyber Infrastructure, or a network that is not logically isolated from high or medium impact BES Cyber Systems.

Rationale

The Removable Media definition is being updated to remove the dependency on ESP and allow for other methods of logical isolation as well as adding SCI as a target of the Removable Media connection.

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System that performs one or more reliability tasks of a functional entity;

- The logical isolation of a high or medium impact BES Cyber System;
- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or
- Shared Cyber Infrastructure of a high or medium impact BES Cyber System.

Rationale

This definition is being modified to remove the dependency on ESP and allow for other methods of logical isolation as well as adding SCI as a target of an incident.

Transient Cyber Asset (TCA)

A Cyber Asset or Virtual Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Shared Cyber Infrastructure associated with high or medium impact BES Cyber Systems,
4. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
5. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
    - BES Cyber Asset,
    - Shared Cyber Infrastructure,
    - Network that is not logically isolated from high or medium impact BES Cyber Systems, or
    - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Rationale

The TCA definition is being updated to remove the dependency on ESP and allow for other methods of logical isolation, as well as adding VCA as a form a TCA can take (and excluding the SCI on which the virtual TCA executes). The intent is to handle VCAs that are created for typical TCA uses but are normally dormant (e.g. a Virtual Machine (VM) with Wireshark for troubleshooting network issues within a virtualized infrastructure). Additionally, SCI was added as a target to which TCA's can be directly connected.

Proposed New Terms

Management Interface

A physical or logical interface of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities.

Rationale

This term is being defined so that requirements can be addressed to SCI and EACMS Management Interfaces. For example, if a network switch is enforcing logical isolation between different logical networks (such as VLANs), it is an EACMS and its Management Interface must be protected (e.g. CIP-005 Requirement R1 Part 1.2)

Management Module

An autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.

Rationale

Management Modules, also known as ILO (Integrated Lights Out), are a type of Management System that can be used to remotely manage hardware (usually including power on/off, remote console access, etc.). This term is being defined such that it can be excluded from the definition of Management System and addressed directly with a requirement (CIP-005 R1.5) to protect access to the Management Interface of the Management Module and to deny access from hosted BES Cyber Systems (tenants) to the Management Module capability of the SCI on which it depends.

Management Systems

Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Cyber Assets or Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.

Rationale

This term is being introduced to target the unique risk for virtualized environments presented by the management 'consoles' for such environments. With 'infrastructure as a service' (IaaS) environments, the management consoles can not only be used to create, but also to destroy or reconfigure virtual servers, networks, switches, firewalls, etc. This intent is to define that capability and then include this within the definition of SCI.

Self-Contained Application (SCA)

Immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment.

Rationale

With the advent of application containers and container orchestration platforms, this definition is being created so that containers and their unique attributes can be addressed in CIP-010 for change management.

Shared Cyber Infrastructure (SCI)

One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.

Rationale

The SCI definition is being created to separate the underlying hardware from the VCAs that it hosts. This allows security requirements to be targeted to SCI to address the unique risks of virtualization and shared hardware. There are many requirements that now include the newly defined term SCI in the "Applicable Systems" column to maintain security level parity with traditional Cyber Assets.

Beyond security level parity with protecting a typical hardware based Cyber Asset, the SCI can have a more significant impact in a virtualized environment since it can host, and therefore impact, multiple virtualized systems. Because of this capability, some additional controls only apply to SCI, such as the management plane isolation required by the proposed CIP-005 R1.5. Addressing these unique risks requires separation of the hardware underlay into a separate definition.

Of note is that shared network devices are not in the scope of this definition. Since network switches and firewalls share their resources by nature, this exclusion avoids pulling all network hardware into scope as SCI. However, network switches and other hardware that does perform logical isolation (such as a network switch configured to logical isolate different VLANs) comes into scope as an EACMS as well and falls under CIP-005 R1.5.

Virtual Cyber Asset (VCA)

A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure or a Cyber Asset.

Rationale

The NERC Glossary definition of Cyber Asset has a direct tie to the hardware on which it relied. This affected the definitions of the “Applicable Systems” terms such as BES Cyber Systems (BCS), EACMS, PACS, and Protected Cyber Assets (PCAs). Because the Reliability Standard is applicable to the aforementioned systems, the control for the Cyber Assets also applies to the hardware. This one-to-one relationship between a Cyber Asset and its underlying hardware is what virtualization intentionally breaks to increase reliability and resiliency by allowing Virtual Cyber Assets to be abstracted from the hardware and therefore able move to any available hardware out of a pool of resources.

The proposed NERC Glossary definition of Virtual Cyber Asset (VCA) allows the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined. The definition of VCA is not inclusive of hardware, and other related definitions (EACMS, PACS, PCA, TCA, etc.) have been updated to allow for VCA versions. With the addition of SCI and revisions to the “Applicable Systems”, there can be one or more virtualized instances (each a VCA) of a BCA, EACMS, PACS or PCA that reside on SCI.

Examples of Virtual Cyber Assets may include, but are not limited to, logical instances of the following:

- Operating Systems (Virtual Machines (VM));
- Networking devices such as switches, routers, and load balancers;
- Security appliances such as firewalls and VPN concentrators; and
- Helper appliances with logical connectivity (such as malware detection, plugins, etc.).

Proposed Retired Terms

Electronic Security Perimeter (ESP)

The logical border surrounding a network to which BES Cyber Systems are connected using a routable Protocol.

Rationale

The Electronic Security Perimeter, while still a valid network security model, is no longer the only prescribed model as CIP-005 now allows other non-perimeter based models in its “logical isolation” paradigm. As such, the glossary term ESP is no longer used within the standard and will move to the inactive section of the NERC glossary. Entities are free to continue use of the term since ESP’s remain a valid method to logically isolate BES Cyber System.

Electronic Access Point (EAP)

A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Rationale

In addition to the rationale for the retirement of ESP, as network security moves deeper into the infrastructure, its no longer necessary to prescribe that network security be performed on a ‘Cyber Asset interface on an ESP’; at one point on a network edge. Zero Trust, for example, highly distributes the network security model and is not perimeter-based. With the added flexibility in CIP-005 to adopt these models in place of the traditional ESP model, the term EAP is no longer prescribed or used within the standards. Entities are free to continue to use the term as it will move to the inactive section of the NERC Glossary.

Proposed Retired Terms

Electronic Security Perimeter (ESP)

The logical border surrounding a network to which BES Cyber Systems are connected using a routable Protocol.

Rationale

The Electronic Security Perimeter, while still a valid network security model, is no longer the only prescribed model as CIP-005 now allows other non-perimeter based models in its “logical isolation” paradigm. As such, the glossary term ESP is no longer used within the standard and will move to the inactive section of the NERC glossary. Entities are free to continue use of the term since ESP’s remain a valid method to logically isolate BES Cyber System.

Electronic Access Point (EAP)

A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Rationale

In addition to the rationale for the retirement of ESP, as network security moves deeper into the infrastructure, its no longer necessary to prescribe that network security be performed on a ‘Cyber Asset interface on an ESP’; at one point on a network edge. Zero Trust, for example, highly distributes the network security model and is not perimeter-based. With the added flexibility in CIP-005 to adopt these models in place of the traditional ESP model, the term EAP is no longer prescribed or used within the standards. Entities are free to continue to use the term as it will move to the inactive section of the NERC Glossary.

Technical Rationale for Exemptions Section

Rationale for Exemption 4.2.3.1

The term ‘Cyber Assets’ was changed to ‘Cyber systems’. Rather than changing this language to a list of all possible forms (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure) as the object of the exemption, the SDT chose to instead use the existing language in the 4.2.3.4 and 4.2.3.5 exemptions such that all five exemptions use ‘systems’ as their object.

Rationale for Exemption 4.2.3.2 and 4.2.3.3

In 4.2.3.2, the term ‘Cyber Assets’ was changed to ‘Cyber systems’. Rather than changing this language to a list of all possible forms (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure) as the object of the exemption, the SDT chose to instead use the existing language in the 4.2.3.4 and 4.2.3.5 exemptions such that all five exemptions use ‘systems’ as their object.
In previous versions of the CIP standards, Cyber Assets associated with communication networks and data communication links between discrete ESP’s were exempt from the scope of the standards. There are two issues raised by virtualization technologies with this exemption:

1. Perimeter-based network security models are no longer the only model available
2. The ability to move workloads or VM’s seamlessly across different sites for increased resiliency can require different sites to be connected without layer 3 ESP’s at each discrete site but with layer 2 adjacency across the sites. In other words, a “Super ESP” as its been historically known is created across the sites, and thus an exemption based on having a discrete layer 3 ESP at each site no longer works to exclude, for example, the network transport equipment belonging to carriers.

The concept of logical isolation in CIP-005 addresses these issues. First, it allows for models other than the perimeter-based model (such as Zero Trust) and it allows for cyber systems associated with the communication links that are logically isolated from the BES Cyber Systems or the Shared Cyber Infrastructure (SCI) to still meet this exemption. A companion requirement has been added to CIP-005-8 (Requirement 1 Part 1.3) to require protecting the data traversing these links that can’t be logically isolated, such as these layer 2 adjacency situations between sites.

Exemption 4.2.3.3 can be viewed as a particular scenario under 4.2.3.2. The SDT is including it to further clarify what is known as the “Super ESP” scenario. Responsible Entities should notice the definition uses the word “between” – when extending logical isolation or a “Super ESP” between geographic locations, CIP-005 requires the protection of the data (typically through encryption) between the relevant PSPs. This exemption will then exempt the related cyber systems “between” those encryption points but does not exclude the endpoints performing the encryption.

DRAFT

Cyber Security — BES Cyber System Categorization

Technical Rationale and Justification for Reliability Standard CIP-002-7

January 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-002-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-002-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-002-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

Requirement R1 Part 1.3

Change Rationale:

The SDT modified Requirement R1 Part 1.3 to include the identification of "assets containing" to include low impact BES Cyber Systems (BCS) as well as assets containing Shared Cyber Infrastructure (SCI) that hosts any portion of a low impact BCS. This modification was made because SCI, which can host multiple BCS, may pose a greater risk to the BES than a single BCS. Additionally, the term Cyber Asset was modified to exclude SCI so that SCI could could be addressed separately from any hosted BCS. Responsible Entities should note that the definition of SCI contains its associated Management Systems, thus an "asset containing" could be a location of the Management System used to manage a distributed SCI.

For example, hypervisors within one SCI may be distributed across numerous assets such as substations, generating sites, or control centers and the Management System for the SCI could be located at yet another location. With this change, the rationale is the "asset" containing the Management System becomes important as it relates to potential impact to the low impact BCS and would be another identified entry on the Responsible Entity's evidence for R1.3 that is later subject to controls in CIP-003 Requirement R2 that parallell those for the asset containing the low impact BCS.

Requirement R1 Part 1.4 – 1.5

Change Rationale:

Requirement R1 Parts 1.4 and 1.5 have been added to require the identification of all SCI that hosts high impact BCS (Part 1.4) and medium impact BCS (Part 1.5). SCI can host not just a single but multiple BCS, Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), Protected Cyber Assets (PCA), etc. of varying impact levels or association to a BCS. As such, they may present a higher level of risk than a single BCS and are called out to be discretely identified.

Attachment 1 – Impact Rating Criteria

Change Rationale:

In the medium impact rating criterion 2.1 referencing shared BCS for commissioned generation, the SDT has proposed a change to incorporate an earlier approved Request For Interpretation (RFI). The RFI was submitted seeking clarification of Criterion 2.1 of Attachment 1 regarding the use of the phrase "shared BES Cyber Systems." The resulting approved interpretation was introduced as Appendix 1 in CIP-002-5.1, and later carried over into CIP-002-6.

The SDT incorporated the interpretation into CIP-002-7 Attachement 1 criterion 2.1 by modifying it to reference "each discrete shared BCS" and removed the RFI from the standard.

Former Background Section from Reliability Standard CIP-002-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a security plan for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the initial scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than “Real-time,” BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement R1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

- **Electronic Access Control or Monitoring Systems (“EACMS”)** – Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.
- **Physical Access Control Systems (“PACS”)** – Examples include: authentication servers, card systems, and badge control systems.
- **Protected Cyber Assets (“PCA”)** – Examples include, to the extent they are within the ESP: file servers, FTP servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

Technical Rational for Reliability Standard CIP-002-6

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-002-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-6 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-6. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-6

CIP-002-6 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, “…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES.”

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-6. The concept includes a number of named BES reliability operating services. These named services include:

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)

- Controlling Voltage (Reactive Power)
- Managing Constraints
- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
    - Providing actual reserve generation when called upon (GO,GOP)
    - Monitoring that reserves are sufficient (BA)
- Governor Response
    - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
    - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
    - Zone protection for breaker failure (DP, TO, TOP)

  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)

  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL’s & IROL’s (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)

- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

When the drafting team uses the term "Facilities," there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as, "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-6, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.

In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.

It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating

No additional evaluation is necessary for BES Cyber Systems that have already been identified as high impact.

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

  The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e. that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional

Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.
- Criterion 2.9 categorizes BES Cyber Systems for Remedial Action Schemes as medium impact. Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.
- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.
- Criterion 2.13 categorizes as medium impact those BA Control Centers that “control” 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.
- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the “Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface.” This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:
  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

Additionally, in Attachment 1 of NERC's "Integrated Risk Assessment Approach – Refinement to Severity Risk Index" document, the report used an average MVA line loading based on kV rating:

- 230 kV –> 700 MVA
- 345 kV –> 1,300 MVA
- 500 kV –> 2,000 MVA
- 765 kV –> 3,000 MVA

In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

- For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.
- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4.: there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.
- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.
- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.
- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.
- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the

aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource (“LaaR”) Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes medium impact BES Cyber Systems associated with Control Centers and backup Control Centers, including associated data centers, that monitor and control BES Transmission Lines with an aggregate weighted value of 6000 or higher, and that have not already been included in Part 1. The drafting team included additional qualifications in this criterion that would ensure the required level of impact to the BES is defined and a risk threshold associated to establish a floor for applicable medium impact BES Cyber Systems.

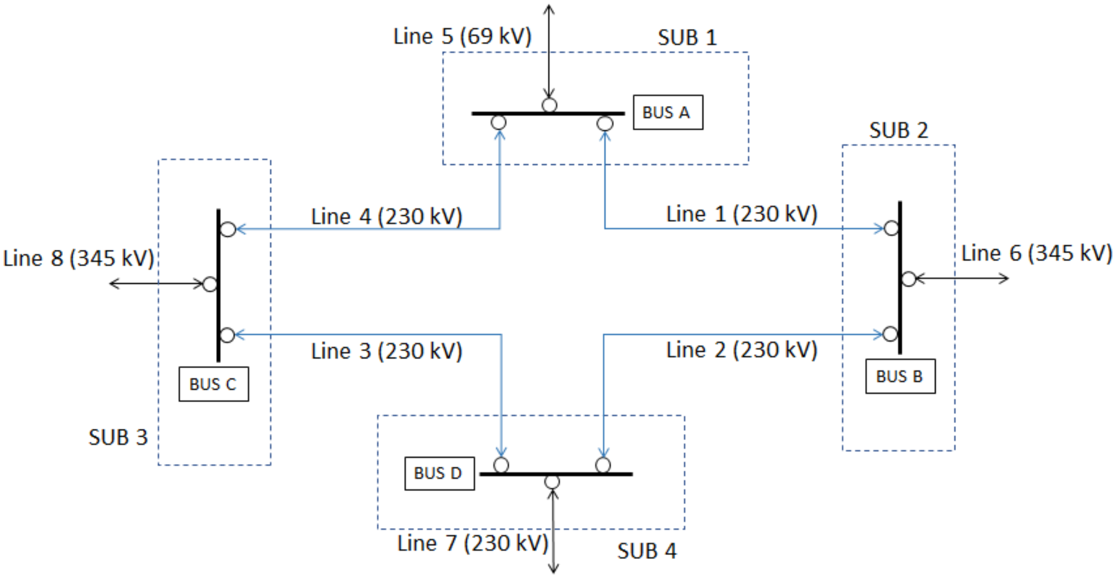
  The total aggregated weighted value is used to account for the impact to the BES. The 6000 aggregate weighted value threshold defined in criterion 2.12 provides a sufficient differentiation for medium and low impact BES Cyber Systems associated with Control Centers that monitor and control BES Transmission Lines. SDT analysis of Transmission Control Centers validated that those facilities that may have significant impact are categorized at an appropriate level commensurate with the associated risk.

  In the terms of applicable BES Transmission Lines, the following should be considered:

  - All BES Transmission Lines that are energized at voltages between 100 kV and 499 kV and are monitored and controlled by a Control Center, including associated data center(s).
  - All BES Transmission Lines, including those that connect to neighboring entities, that are monitored and controlled by the Responsible Entity’s Control Center, including associated data center(s).
  - Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line. For example, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
  - Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. For example, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

  Criterion 2.12 Examples:

In example 1 below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.



Example 1

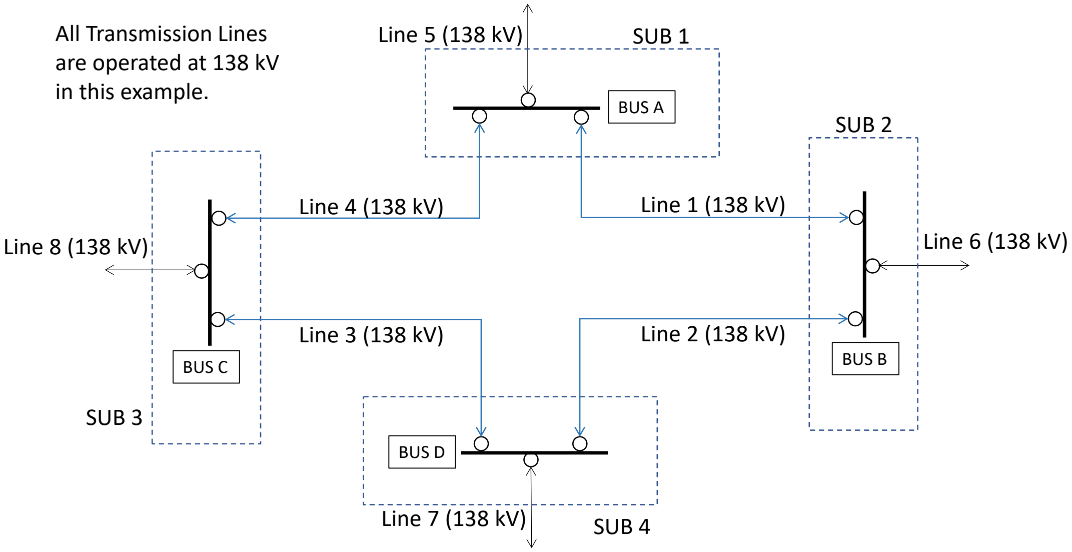
The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 6100, which is above the minimum threshold for the medium impact rating required in Criterion 2.12. In accordance with Criterion 2.12, the BES Cyber System(s) associated with the Control Center should be categorized as medium impact BES Cyber System(s).

Voltage Value of a Line	Weight Value per Line	Applicable Lines	Weighted Value
less than 100 kV (not applicable)	(not applicable)	Line 5	N/A
100 kV to 199 kV	250	None	0
200 kV to 299 kV	700	Line 1, Line 2, Line 3, Line 4, Line 7	3500
300 kV to 499 kV	1300	Line 6, Line 8	2600
500 kV and above	0	None	0

Calculation

700+700+700+700+700+1300+1300 = 6100

In the additional example below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.



Example 2

The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 2000, which is below the minimum threshold for a medium impact rating required in Criterion 2.12. The BES Cyber System(s) associated with the Control Center in this example should be categorized as a low impact BES Cyber System(s) pursuant to Criterion 3.1.

Voltage Value of a Line	Weight Value per Line	Applicable Lines	Weighted Value
less than 100 kV (not applicable)	(not applicable)	None	N/A
100 kV to 199 kV	250	Line 1, Line 2, Line 3, Line 4, Line 5, Line 6, Line 7, Line 8	2000
200 kV to 299 kV	700	None	0
300 kV to 499 kV	1300	None	0
500 kV and above	0	None	0

Calculation

250+250+250+250+250+250+250+250= 2000

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating

No additional evaluation is necessary for BES Cyber Systems that have already been identified as high or medium impact. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact. Note that low impact BES Cyber Systems do not require discrete identification, only identification of the asset containing the low impact BES Cyber System(s).

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

  Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

  BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in

its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

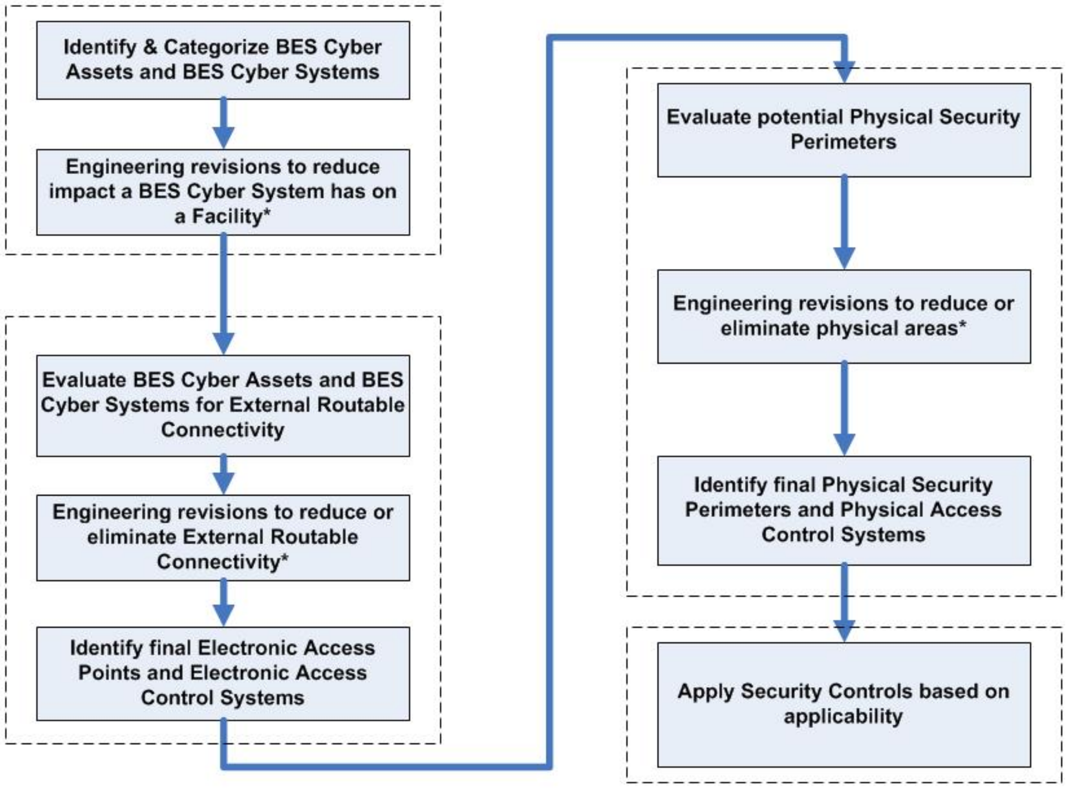
- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.

Overview (Generation Facility)



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Appendix 1

Requirement Number and Text of Requirement

CIP-002-5.1, Requirement R1

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

- i. Control Centers and backup Control Centers;
- ii. Transmission stations and substations;
- iii. Generation resources;
- iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

Attachment 1, Criterion 2.1

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions

Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase “shared BES Cyber Systems.”

The Interpretation Drafting Team identified the following questions in the RFI:

1. Whether the phrase “shared BES Cyber Systems” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

2. Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?
3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

Responses

Question 1: Whether the phrase “shared BES Cyber Systems,” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states “Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…” Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states “*Each BES Cyber System*…associated with any of the following [criteria].” (emphasis added)

Additionally, the Background section of CIP-002-5.1 states that “[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System.” The Background section also provides:

> The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Question 2: Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term “shared” is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.” For criterion 2.2: “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-9

January 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-003-9

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-9. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-9 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document stated, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." document for reference when reading the technical rational that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-9 to align security management control requirements with the virtualization changes.

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-003-9 Requirement R1 for virtualization, the SDT added “and associated SCI” to specified impact levels of BCS.

Requirement R2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-9 to align security management control requirements with the virtualization changes.

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-003-9 Requirement R2 for virtualization, the SDT added “and their associated SCI” to the low impact BCS and included the same exclusions to require a discrete list, to the low impact BCS.

Attachment 1 Section 2

Rationale

To ensure SCI hosting a low impact BCS is afforded equal physical security controls as the BCS, the SDT added “the asset or the locations of the SCI hosting low impact BES Cyber Assets within the asset.”

Additionally, to ensure virtual infrastructure providing electronic access controls for the low impact BCS is afforded equal physical security controls as the physical Cyber Assets that provide electronic access controls for the low impact BCS, the SDT modified this section to include the Virtual Cyber Asset (VCA) where only Cyber Assets had previously been listed.

Attachment 1 Section 3

Rationale

To ensure an asset containing a low impact BCS or an SCI hosting a low impact BCS is afforded equal electronic access controls as the low impact BCS, the SDT added “or its associated SCI” as identified in CIP-002.

Attachment 1 Section 3 Part 3.1

Rationale

Part 3.1(i) To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a system(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term system(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Part 3.1(ii) To ensure only necessary inbound and outbound electronic access is permitted for SCI hosting a low impact BCS just as is required for access control to the low impact BCS, the SDT adjusted the language to include communications that are between SCI hosting a low impact BCS and a system(s) outside the asset(s) containing the SCI hosting a low impact BCS

Part 3.1 (iii) To ensure SCI associated to low impact BCS is afforded equal electronic access controls for routable communications entering or leaving the asset containing the low impact BCS, the SDT added “or their associated SCI” to the low impact BCS.

Attachment 1 Section 3 Part 3.2

Rationale

To ensure SCI associated to low impact BCS are afforded equal electronic access controls for Dial-up Connectivity, the SDT added “or their associated SCI” to the low impact BCS. Per VCA capability was included in addition to per Cyber Asset capability to accommodate for incapability of both physical and virtual aspects of the low impact BCS or its associated SCI.

Attachment 1 Section 5

Rationale

To ensure SCI associated with low impact BCS are afforded equal mitigations from the introduction of malicious code as the low impact BCS, the SDT added “or its associated SCI” to the low impact BCS.

Attachment 1 Section 5 Part 5.2

Rationale

To ensure SCI associated with low impact BCS are afforded equal protections when a TCA managed by a party other than the Responsible Entity is used, the SDT added “or its associated SCI” to the low impact BCS in Attachment 1 Section 5 Part 5.2.1.

Attachment 1 Section 5 Part 5.3

Rationale

To ensure SCI associated with low impact BCS are afforded equal protections from malicious code when using Removable Media, the SDT added “or its associated SCI” to the low impact BCS in Attachment 1 Section 5 Parts 5.3.1 & 5.3.2.

Former Background Section from Reliability Standard CIP-003-8

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Technical Rational for Reliability Standard CIP-003-8

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-003-8 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control

- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity’s security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.)

or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only “necessary” inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for “necessary” inbound and outbound electronic access controls may be documented within the Responsible Entity’s cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

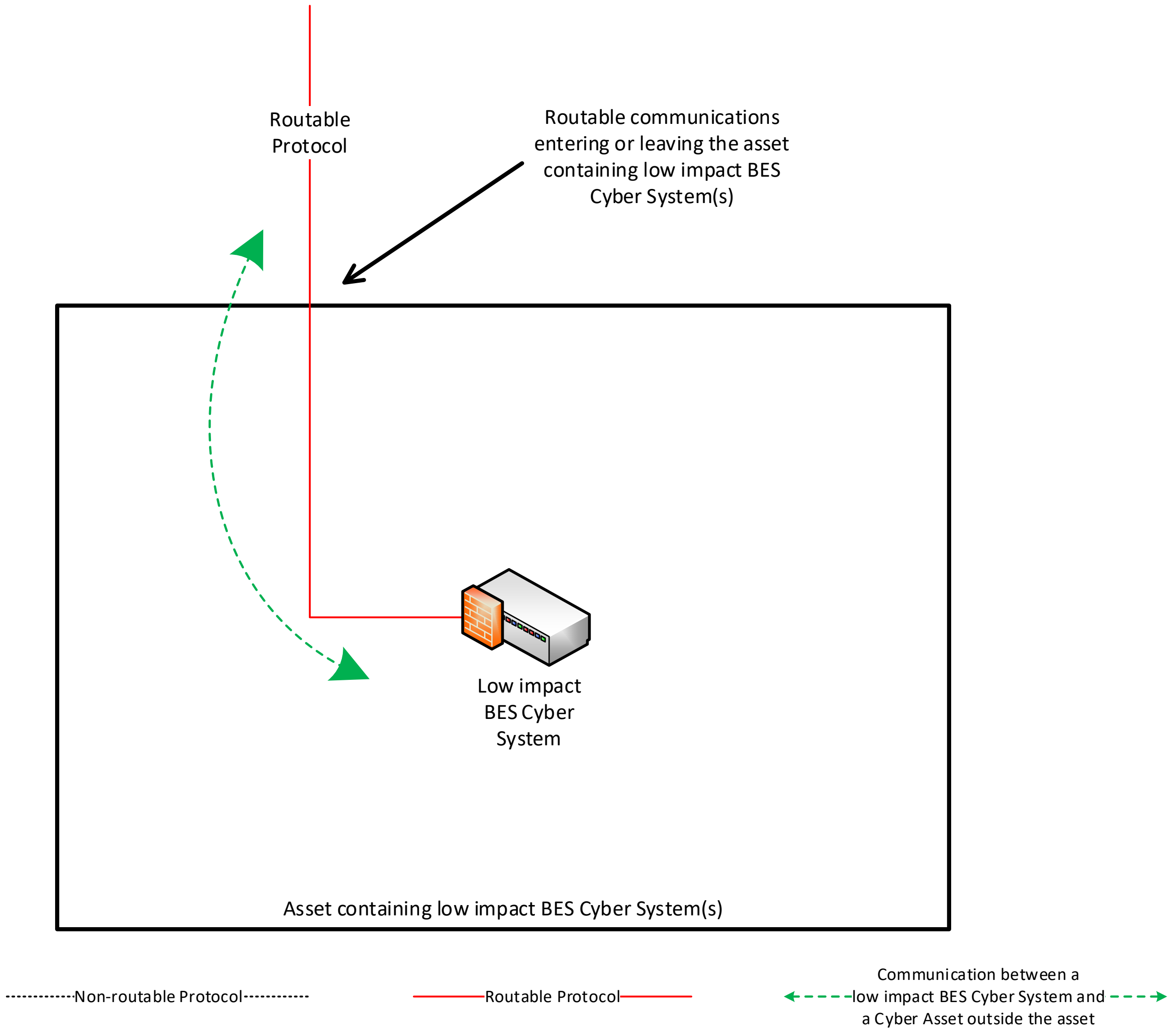
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

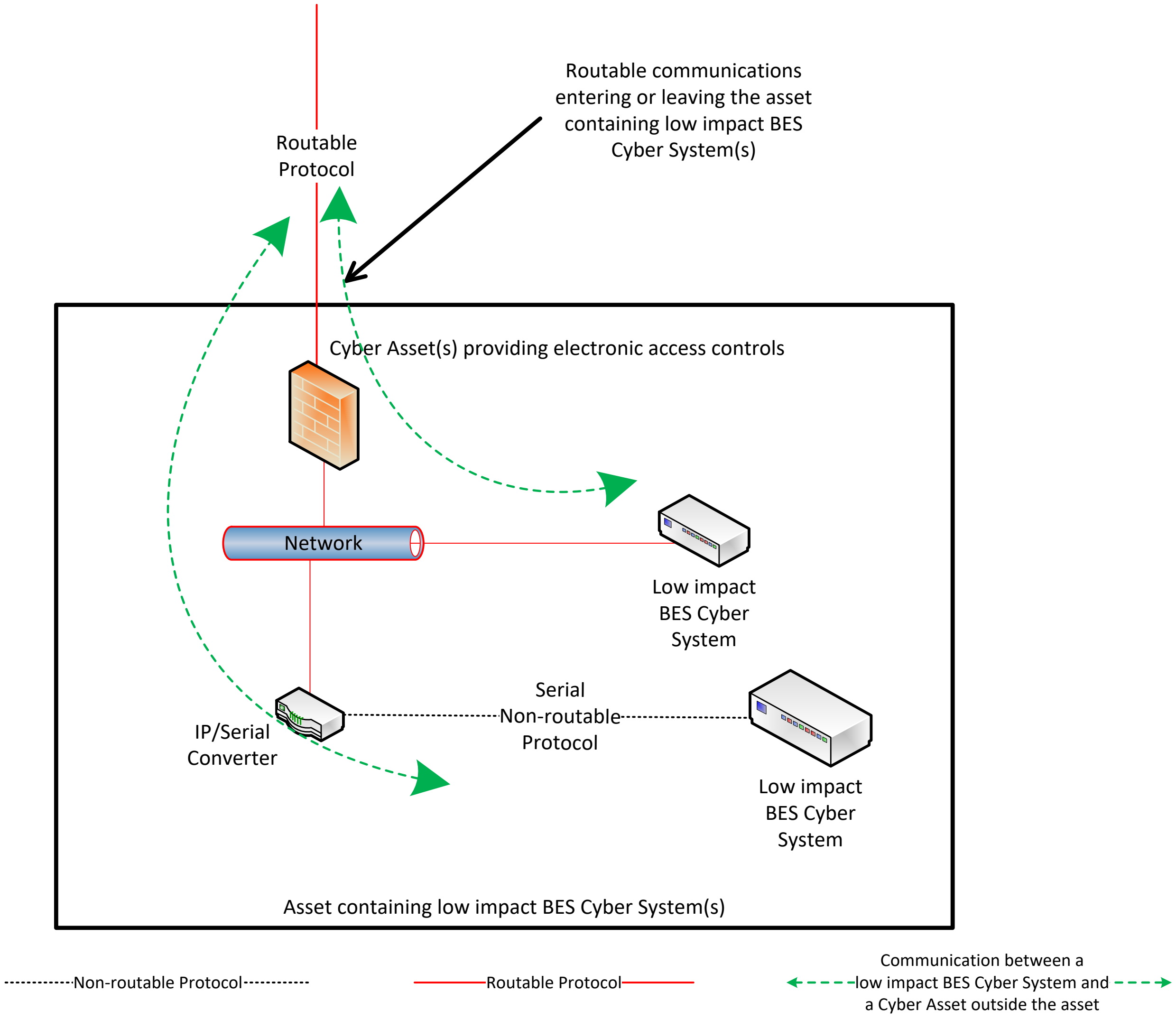
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

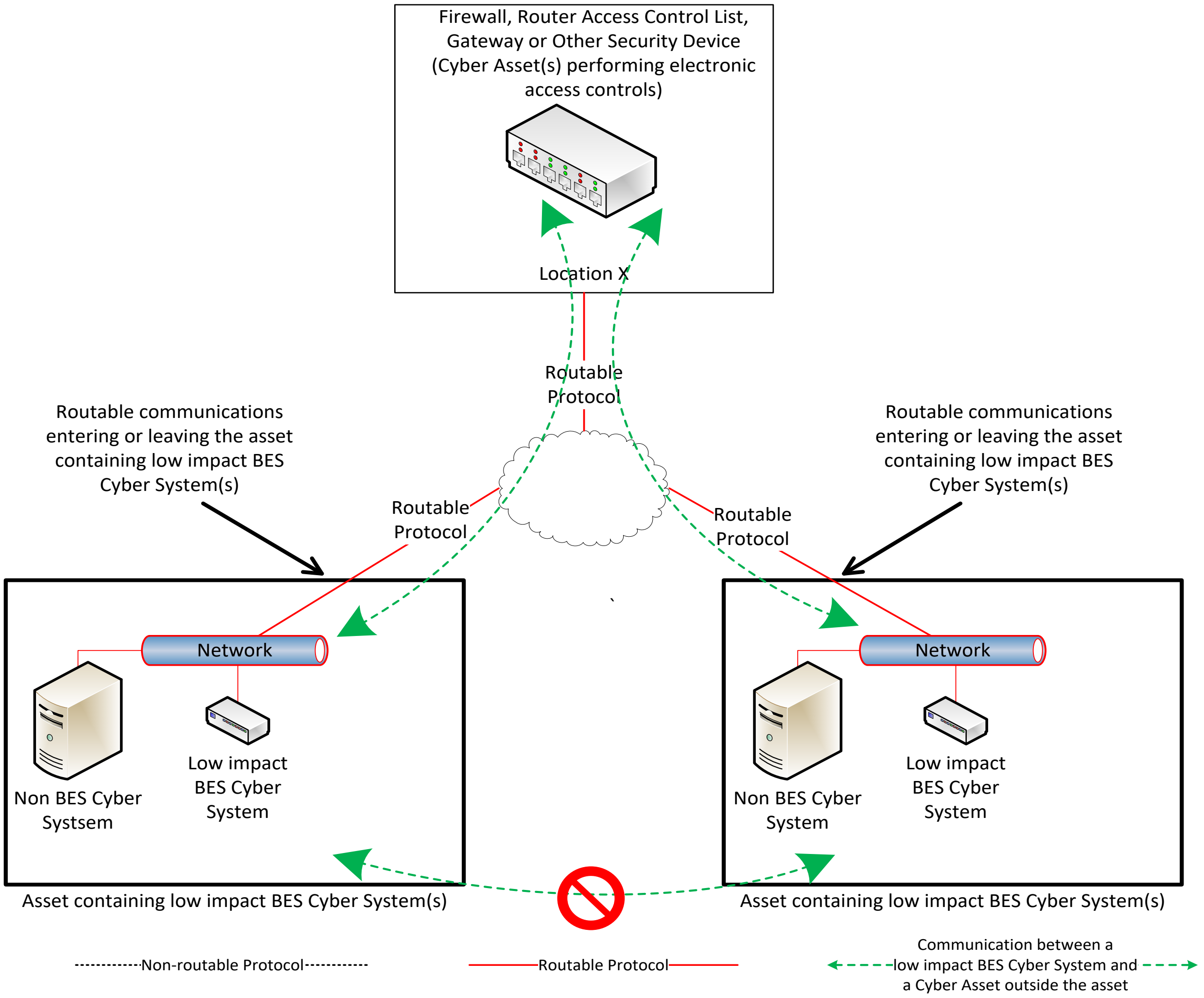
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

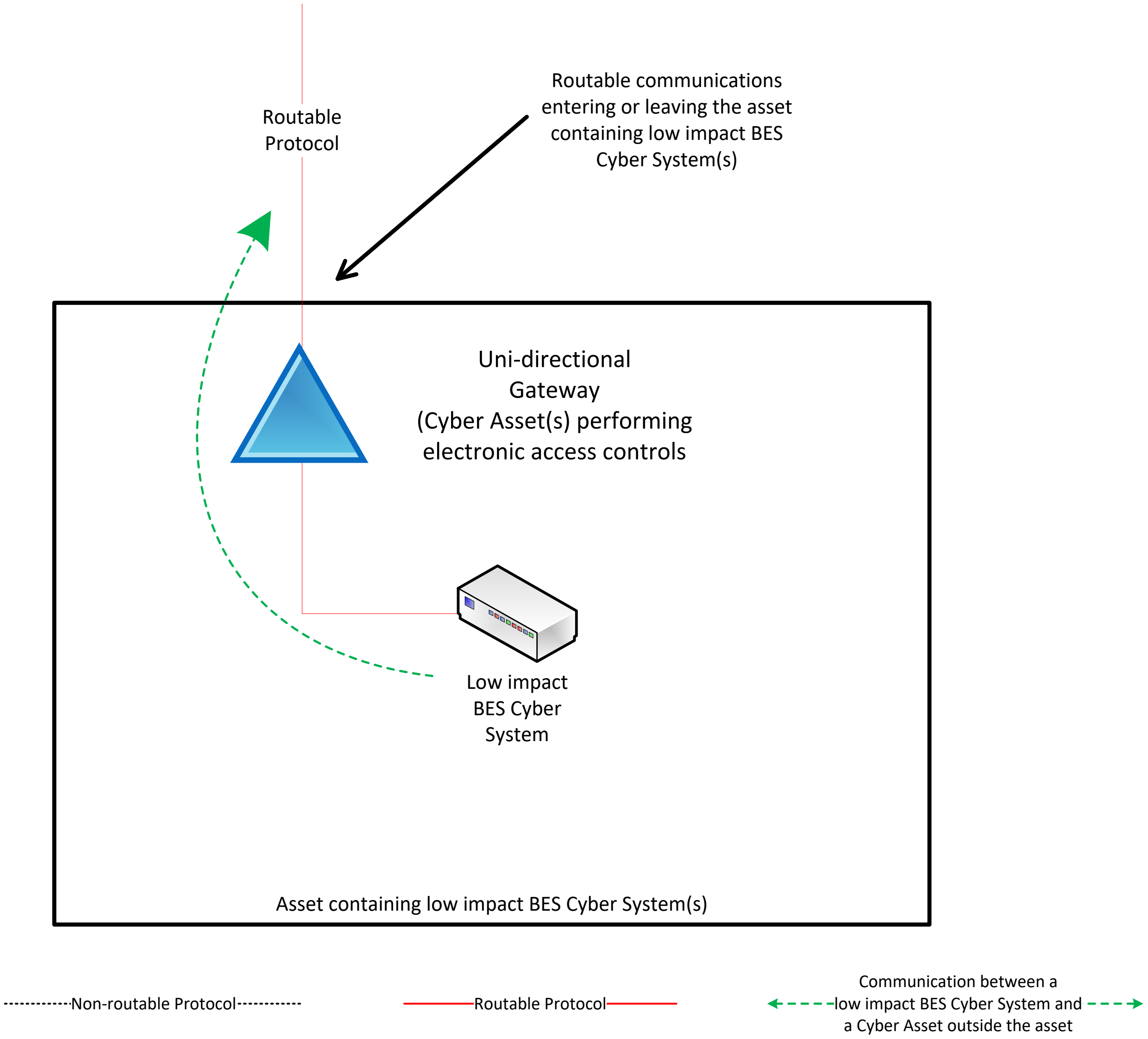
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

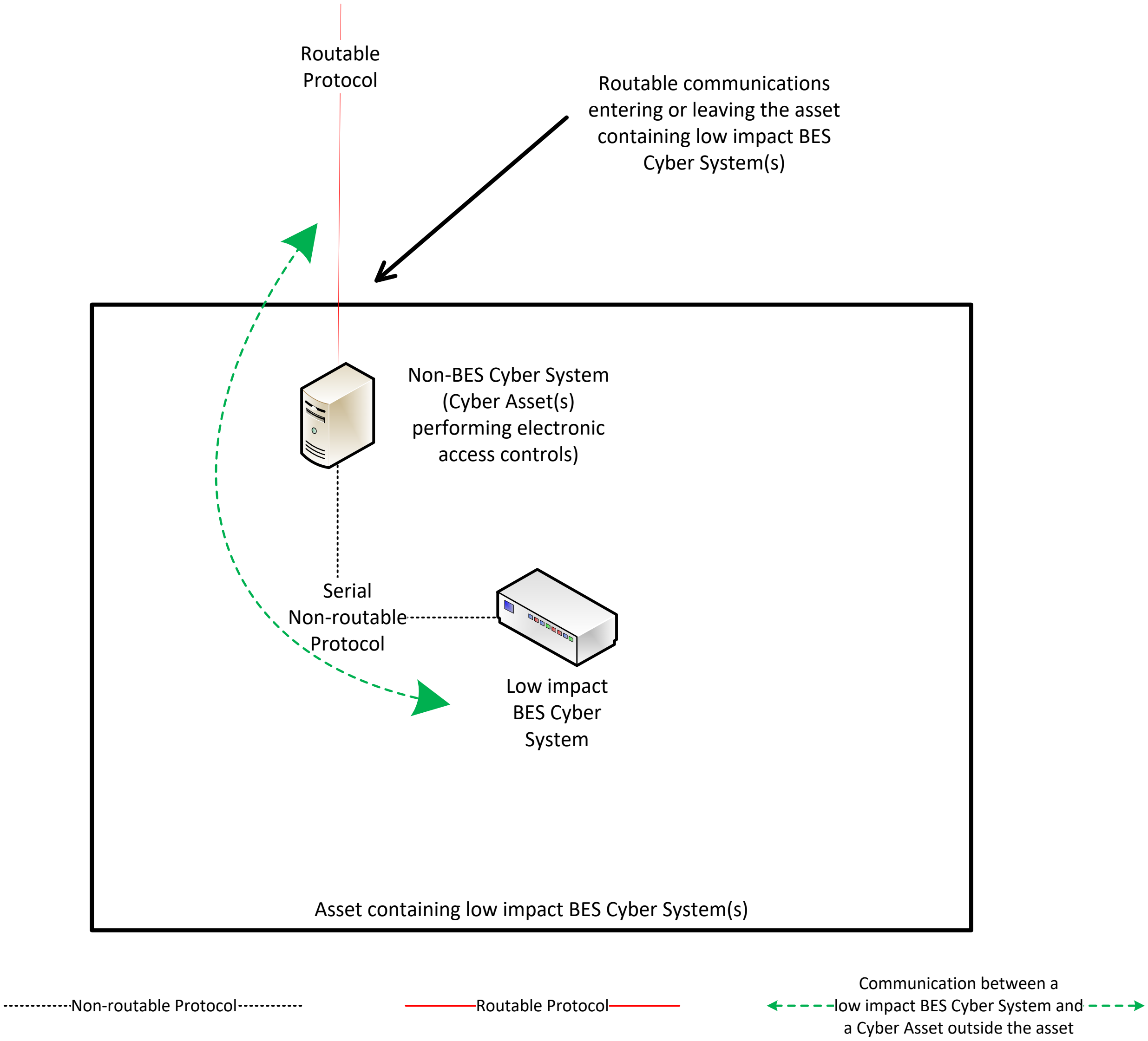
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a “one-way” (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

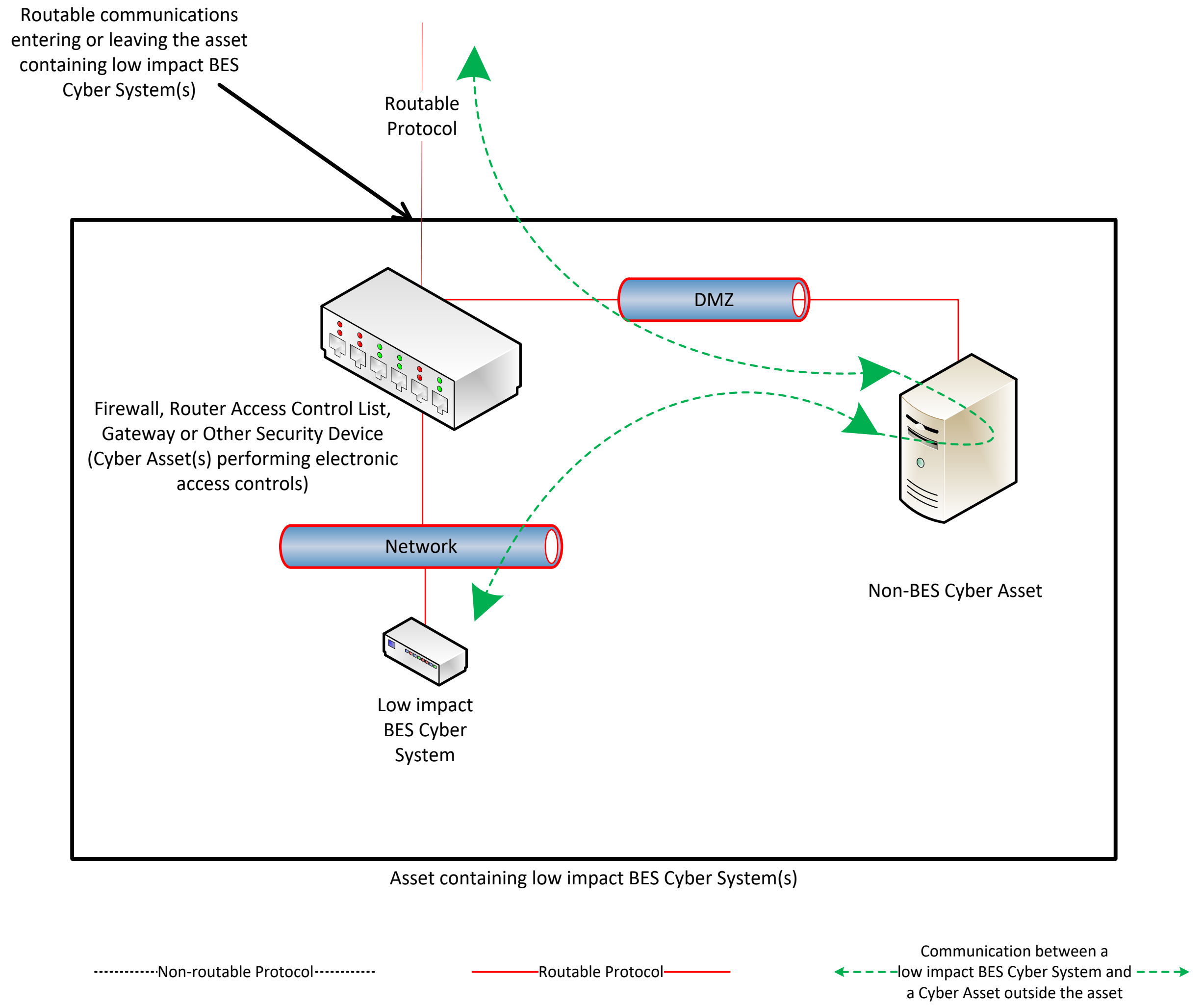
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

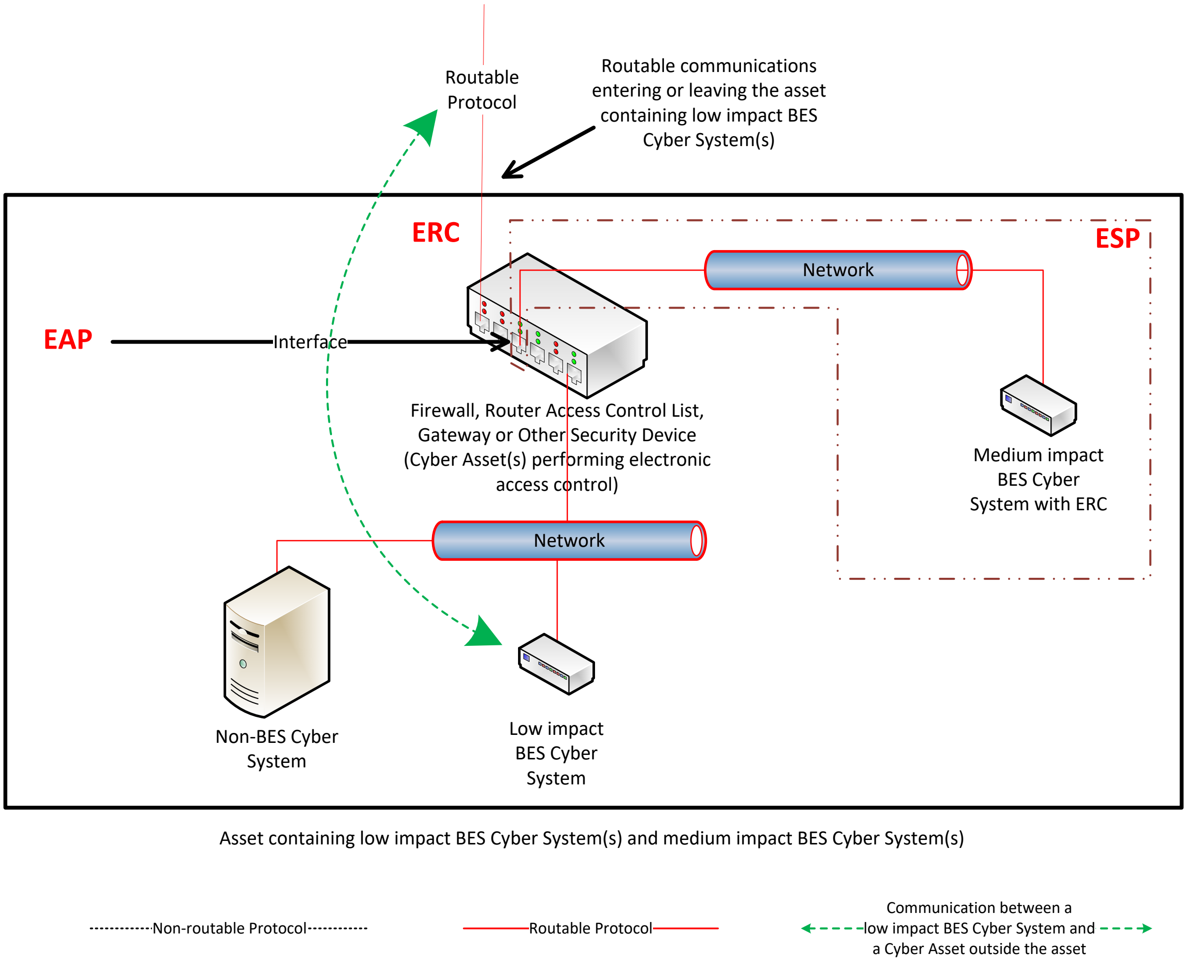
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.



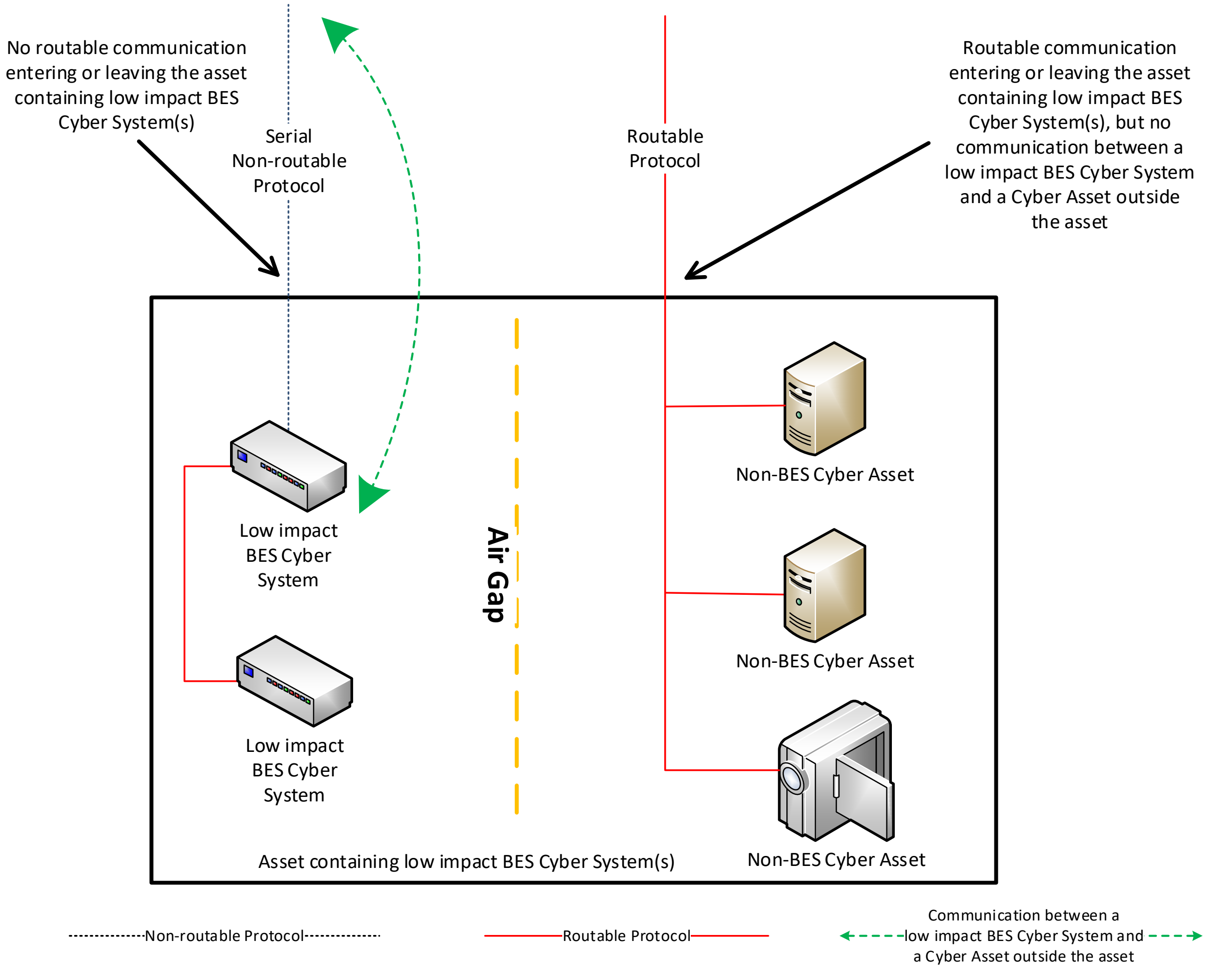
Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).

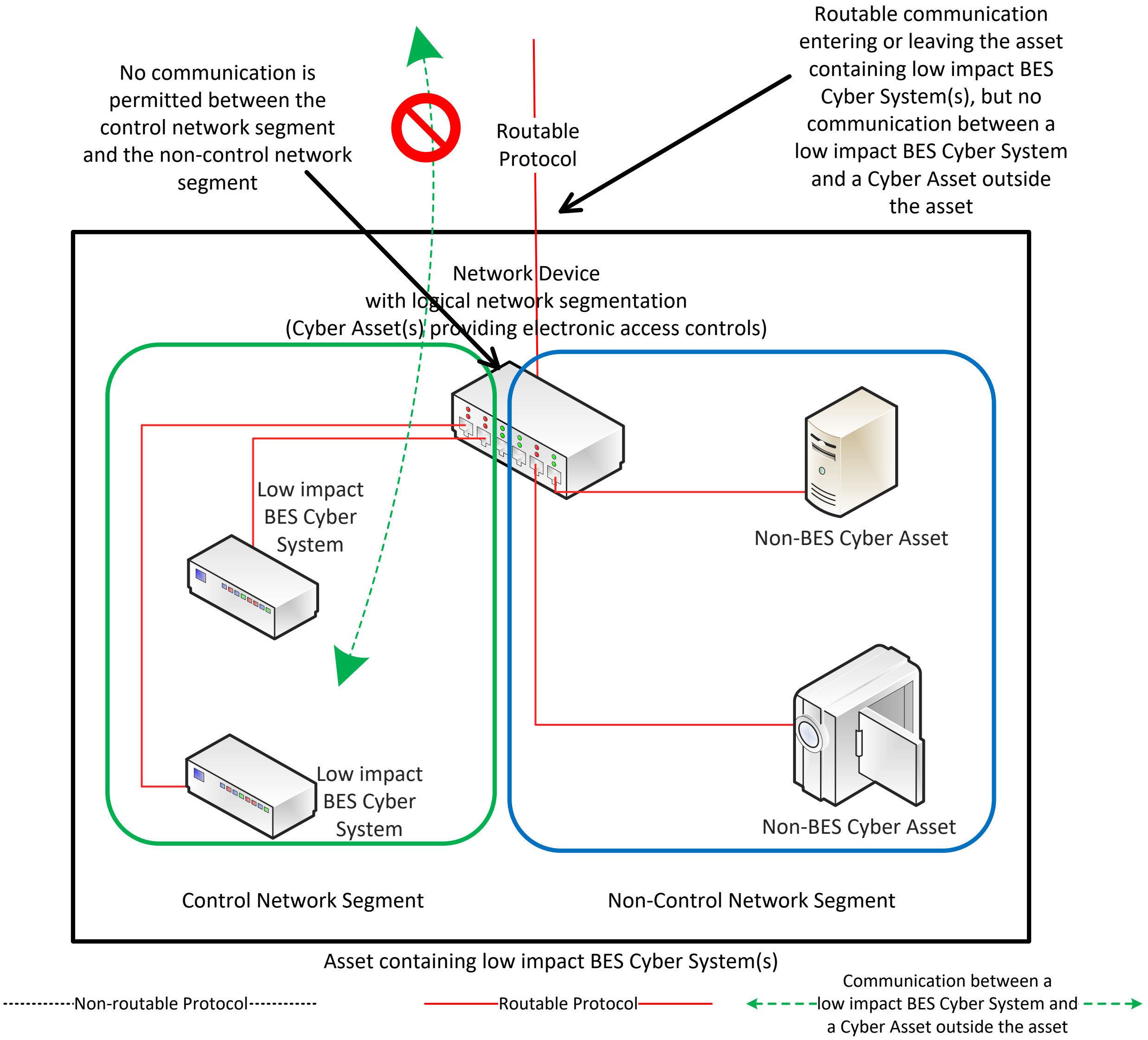
Section 1.



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

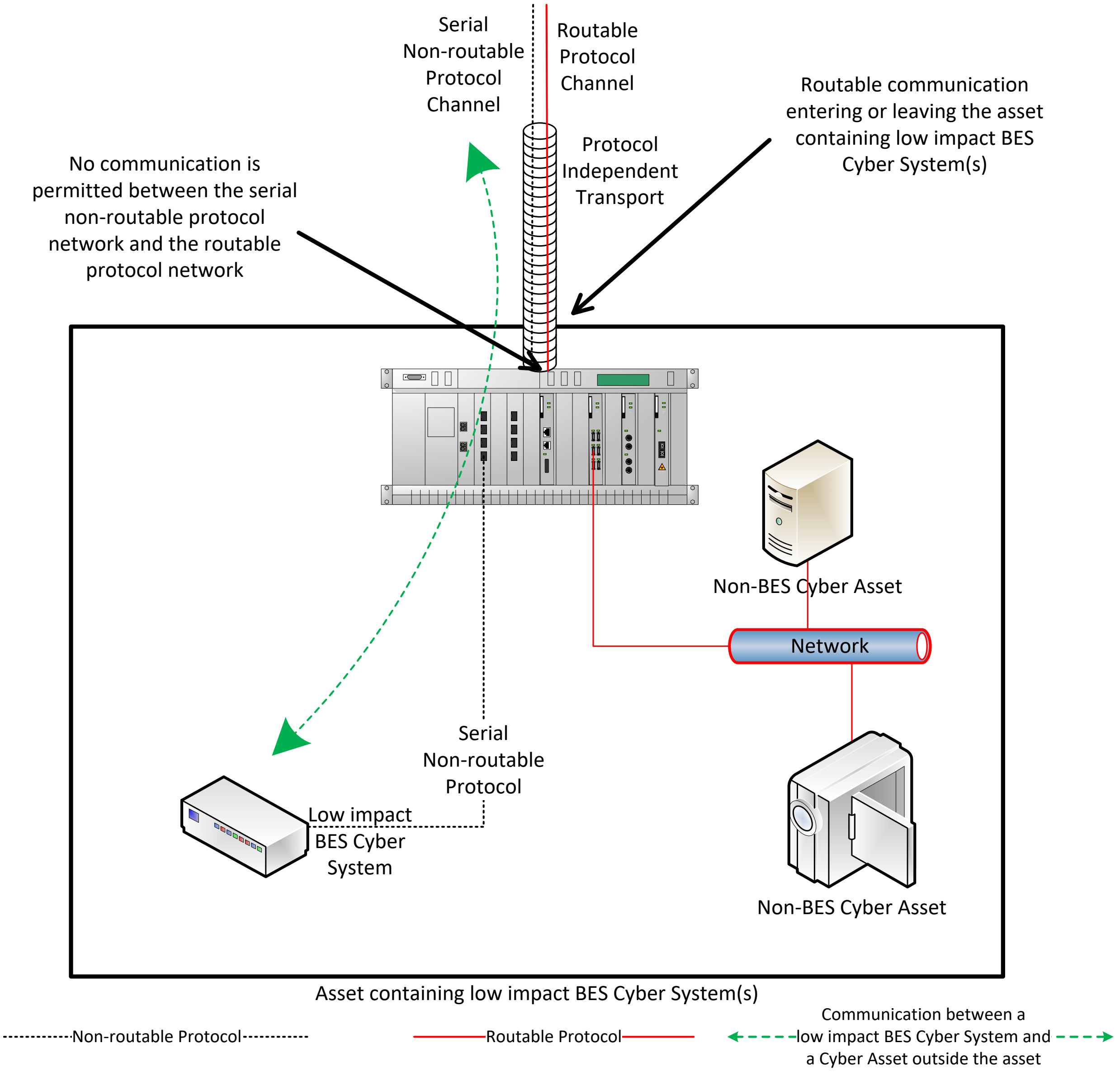
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity’s response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, “A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.” The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation
The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability
As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.

- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2.1: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.

---

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Section 5.2.2: The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):
Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-7

January 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-004-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-004-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the issues identified by the V5TAG was virtualization. The V5TAG Transfer document states, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." Document for reference when reading the technical rationale that follows.

Requirement R1-R5

General Considerations

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-004-7 to align personnel and training requirements with the virtualization changes.

Requirement R3 Part 3.5

Summary of Changes:

A CIP Exceptional Circumstance was added as an exception to processes to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed prior to granting authorized electronic access and authorized unescorted physical access.

Change Rationale:

The SDT determined Responsible Entities cannot require personnel risk assessments for first responders prior to granting them authorized unescorted physical access during certain conditions that qualify as CIP Exceptional Circumstances.

Former Background Section from Reliability Standard CIP-004-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]." The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program.

However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

The following conventions are used in the “Applicable Systems” column as described. High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-004-6

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

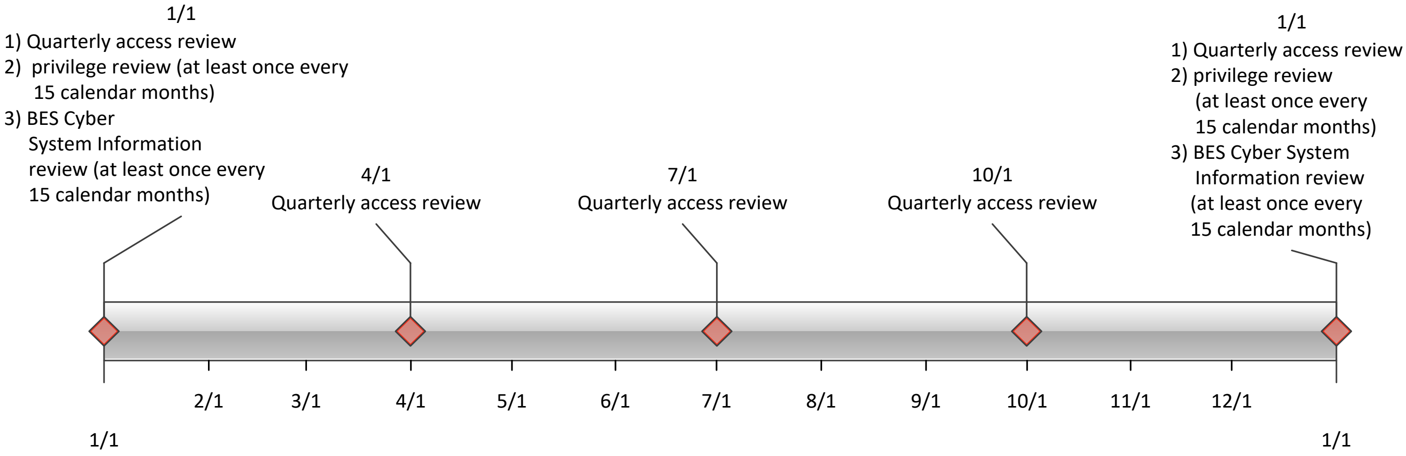
A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.



Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. “Provisioning” should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity’s policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing “immediate” revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security – BES Cyber System Logical Isolation

Technical Rationale and Justification for Reliability Standard CIP-005-8

January 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-005-8

Introduction

This document is the technical rationale and justification for Reliability Standard CIP-005. It includes the rationale for changes in the current proposed version (CIP-005-8) as well as previous versions of the standard. The intent of this document is to provide stakeholders and the ERO Enterprise with an understanding of the revisions and the technical concepts of the Reliability Standard as well as the rationale for such revisions, both the currently proposed and historical revisions from previous versions and SDTs.

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005-8 and the definitions of Cyber Asset and Electronic Access Point (EAP) that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

Summary

The Project 2016-02 Standard Drafting Team (SDT) proposal accommodates for increasing use of virtualization and other technology innovation. The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards, but also to better position the CIP standards to be applicable to additional future technological innovation while, to the extent possible, maintaining backwards compatibility.

The title and purpose of CIP-005-8 changed from Electronic Security Perimeters (ESP) to Logical Isolation. Virtualization is enabling models for network security (such as "zero trust") that are not perimeter based. These innovations are the reason behind the move to a more flexible logical isolation basis for the standard since an ESP is now becoming one option among others. ESP and EAP implementations remain a popular and valid option well into the future and are one method for allowing only necessary and controlled communications while logically isolating all other communications. CIP-005-8 now focuses on this logical isolation such that high and medium impact BES Cyber Systems (BCS) must be "logically isolated" from all other systems (regardless of protocol) to replace the routable protocol-based ESP requirement as the solitary method that may be used.

Another concept introduced within CIP-005-8 is shared infrastructure. With the introduction of hardware (servers, storage, networks) as a generic infrastructure fabric on top of which virtual cyber systems, networks, and storage locations are built, the need to logically isolate cyber systems from others of different trust levels must move beyond a ‘routable protocol only’ separation. In these virtualized environments where shared infrastructure (hardware) is used, a risk of side channel attacks exists where, for example, a low impact BCS that shares CPU or memory with a high impact BCS and could be used to attack the high impact BCS through hardware-based vulnerabilities. CIP-005-8 mitigates this risk by either:

- Using affinity controls within the virtualization environment to configure the hypervisor(s) to disallow Virtual Cyber Assets (VCA) in these differing trust levels to simultaneously exist or execute on the same hardware underlay CPU and memory, or
- Treating all VCA that can simultaneously share the same CPU or memory as Protected Cyber Assets (PCA) of the highest impact system (high watermarking).

Additionally, the SDT is proposing a new requirement (CIP-005-8 Requirement R1 Part 1.5) to separate the management plane of the Shared Cyber Infrastructure (SCI) from the data plane. This is needed to ensure the reliability and security of the management plane as this is where the logical isolation is configured, as well as where the VCAs themselves are created or deleted.

CIP-005-8 also introduces exemptions and requirements for extending logical isolation or ESPs across different Physical Security Perimeters (PSP) (formerly known as “Super ESPs”). This can allow entities to extend a network to replicate data at high speed between two virtualization infrastructures (defined as SCI) or two databases in two different locations to improve the resilience and reliability of BCS. Requirement 1 Part 1.3 within CIP-005-8 requires that data traversing these “Super ESPs” be protected to preserve its integrity and confidentiality.

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in “CIP Definitions and Exemptions Technical Rationale” document for reference when reading the technical rational that follows.

Requirement R1 General Considerations

Logical Isolation

The title and purpose of CIP-005-8 changed from ESPs to Logical Isolation. Isolation methods such as ESPs and EAPs remain a valid option and are one method for implementing logical isolation. However, virtualization technologies present other equally effective methods than a perimeter-based solution that deals only with layer 3 routable protocols at a network boundary. Virtualization and its accompanying SCI have other characteristics such as shared hypervisors, shared storage, shared virtual networks and switches, all of which pose different security concerns but also have their own security controls. To adapt to these changes, CIP-005-8 focuses on an objective-based requirement (in Requirement R1 Part 1.1) for logical isolation.

CIP-005-8 Requirement R1 does not require logical isolation such that BCS must be completely isolated from each other if communication between them is needed. While allowing only necessary network communication between two systems, it requires “logical isolation” of all other unnecessary communication.

Shared infrastructure and “Mixed Trust” Risks

For virtualized environments where shared infrastructure (hardware) is used, a risk of side channel attacks exists. Virtualization allows disparate workloads of what could be differing impact or trust levels to execute on the same CPUs and share the same memory (i.e. RAM) within the infrastructure. There are vulnerabilities that are directly related to sharing hardware such as Spectre, Meltdown, and Rowhammer. Rowhammer, for example concerns processes sharing certain forms of hardware memory. Repeated writing of bits in one process could flip bits in a process in adjacent physical memory. This type of vulnerability is one of the unique risks of SCI.

As this class of vulnerability is specifically about processes executing side by side on the same CPU or memory chips of SCI, the risk of these vulnerabilities is being mitigated in CIP-005-8 by either:

- Declaring the VCAs that share CPU or memory or are within the same logical isolation with a BCS as associated PCAs which will require they meet the same security requirements (high water marking); or
- Configuring the virtualization infrastructure to place VCAs of differing impact or trust levels into differing isolation methods and configuring affinity controls to these zones such that hypervisors do not allow workloads in these differing zones to simultaneously exist or execute on the same hypervisor.

Assets with Multiple Classifications (PCA, EACMS, Intermediate System, SCI, etc.)

The definitions created in support of the CIP Standards have historically included overlap. In this current version of CIP-005-8, the definition of PCA is updated with conforming changes that include VCA, as well as those that share CPU or memory with BCS. Additional definitions such as SCI and VCA will add to the possibility of additional instances of assets or systems meeting multiple definitions, such as EACMS that are also PCA, or SCI.

These definitions are used in both the Applicable Systems column as well as within the requirement language. The fact that one asset or system may have multiple classifications does not pose a significant challenge as long as the Responsible Entity ensures that all requirements that pertain to ANY of the classifications are applied. In other words, if an asset or system meets both the SCI and the EACMS definition, requirements that apply to either definition are applicable.

Requirement R1

Rationale

Requirement R1 is designed to implement various forms of logical isolation between systems such that only necessary communication is allowed between them. There are other network security models available now (such as zero trust) that can accomplish this security objective that are not perimeter based and control these communications only at various discrete points on a VCA or hosting SCI through either software-based policy or interface configuration.. However, the ESP model continues unchanged as CIP-005-8 Requirement R1 moves to an objective-based requirement that the ESP/EAP model can meet as well.

Requirement R1 Part 1.1:

Rationale

This requirement part is a combination of the first three requirement parts in the former CIP-005-7 version of the standard. Virtualization technologies introduce multiple additional methods to isolate systems and communications, beyond the ESP/EAP perimeter-based model. This requirement part is now objective-based and does not prescribe one method of controlling communications to applicable systems and logically isolating all other communications.

By moving to an objective-based requirement, ESP-based models may still meet the objective. The “or as a group” phrase within the requirement part allows for the protection of a group of applicable systems with an ESP/EAP model in order to permit only needed communications to and from those systems while logically isolating (deny by default) all other communications. While the definitions of ESP and EAP will move to inactive status in the retired section of the NERC Glossary of Terms upon the effective date of CIP-005-8, these former terms may still be used by registered entities for perimeter-based architectures to allow entities to continue to use these terms without having to update documentation.

The objective-based requirement allows for other models as well, such as zero trust architectures. Such models are not based on perimeter security that controls communications at a network boundary. Communications are authorized by policy enforcement points throughout the infrastructure. In this model, network security is less topology based and more policy based and is used to protect communication at a very granular level (an individual system or even process level).

While zero-trust architectures are an emerging model, the objective-based requirement also allows for hybrid models that are various combinations of perimeter-based and zero trust architectures. As technology changes, this requirement is flexible as to how the objective is met.

The obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by any required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein in this situation.

Requirement R1 Part 1.2:

Rationale

The SDT is proposing a new Requirement, CIP-005-8 Requirement R1, Part 1.2. The purpose of this new Requirement is to require the separation of the Management Systems of SCI from systems that are not Management Systems. In essence to deny tenant systems hosted on the SCI the ability to communicate with Management Systems.

As virtualized servers, networks, switches, firewalls, and storage are logical constructs, controlling communications to the management of these systems becomes imperative. Communication with the Management Systems and Management Interfaces can allow users to create, modify, or delete objects or entire infrastructures, or move objects from one network to another. Therefore, administrative level or “management access” to the SCI is critical to the security and reliability of the hosted systems. By isolating the Management Systems and Management Interfaces of these devices from the larger audience of users that can communicate with the hosted tenant systems, the attack surface of the SCI is reduced to the group of users with the administrative functions.

As the same technologies used in on-premise virtualization are used by cloud vendors hosting systems from many different customers, the methods used to separate the management plane from the data plane developed quickly as systems moving to the cloud increased. For a cloud-based hosting facility to be successful, the tenants must share hardware resources (SCI as defined here) but have no ability to access or modify other tenants or their configuration. Cloud technology was forced to enhance existing methods and develop new methods to accomplish this separation. SCI presents the same issue for in-house (on-premise) virtualization environments to prevent users of various systems hosted on the SCI from affecting each other or the SCI’s configuration. CIP-005-8 Requirement R1 Part 1.2 will mitigate that issue by bringing the isolation of the Management Systems and Management Interfaces into the scope of the CIP standards.

Requirement R1 Part 1.3:

Rationale

Requirement R1 Part 1.3 was written to address the issue of “Super ESPs” which extend a single ESP beyond one PSP. This Requirement may also apply to virtualized environments that implement network adjacency to allow workloads to automatically move from one physical location to another to increase BCS resiliency.

A security gap was identified that dealt with the potential for data to traverse a connection that uses third-party communications equipment, which is excluded from the CIP Standards. In order to close this security gap, the SDT chose to create Requirement R1 Part 1.3 to enforce confidentiality and integrity controls (such as encryption) on the data that traverses PSPs that are within the same logical isolation. In this case where communication equipment is used to extend a single ESP to more than one PSP, the confidentiality and integrity controls required in CIP-005-8 Requirement R1 Part 1.3 isolate any protected data from access through the communications equipment used to extend the logical isolation, therefore mitigating the threat from third-party communications equipment in use.

This Requirement Part applies to the data that traverses between PSPs. The SDT also combined CIP-006-6 Requirement R1 Part 1.10) into this Requirement Part because cabling and non-programmable communication components that are not protected within a PSP are considered within the CIP-005-8 Requirement R1 Part 1.1 logical isolation. The intent is to protect data moving across the state as well as data traversing cabling that crosses the hall outside of the PSP.

The requirement language specifically exempts the data that falls under CIP-012 Requirements in order to avoid the potential for double jeopardy as well as the time-sensitive protection or control functions as described in CIP-005-8 Requirement R1 Part 1.1 above.

The SDT chose to include “SCI hosting…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in BCS, EACMS, Physical Access Control Systems (PACS) or PCA. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset’s supporting hardware’s impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCA, and are therefore applicable.

Requirement R1 Part 1.4:

Rationale

The SDT chose to include “SCI hosting…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the Shared Cyber Infrastructure, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset’s supporting hardware’s impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and are therefore applicable.

Requirement R1 Part 1.5:

Rationale

The SDT made conforming changes to specify that the malicious communication detection is for Internet Protocol (IP) based traffic that enters or leaves the required logical isolation in order to not prescribe a perimeter-based model.

The SDT chose to include “SCI hosting…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset’s supporting hardware’s impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and are therefore applicable.

Requirement R2:

General Considerations for Requirement R2.

External Routable Connectivity (ERC) and Interactive Remote Access (IRA)

ERC has been used in the CIP standards for different purposes, including:

1. Establishing when EAPs are required (CIP-005-7)
2. Limiting scope of ~38 requirement parts to those locations that have a high enough level of remote connectivity to support the requirement

The move to the more objective-based requirements shifts the obligation away from implementing access controls at a defined cyber asset interface point (or by former definition, EAP). The objective can now be accomplished without dictating any architecture or access control method, thus eliminating ERC’s role in determining EAPs. However, ERC is still needed as a scoping mechanism for the vast scale of systems and their components within the geographically distributed BES locations. Many requirement parts should be scoped based on whether the system has ERC for the following reasons:

- The risk is increased for systems with ERC. The requirement should apply to those BCS with an increased attack surface and risk due to their connectivity/accessibility.
- Locations that have connectivity such as non-routable serial leased circuits should not have to increase their level of remote connectivity and attack surface to meet security requirements. For example, it would not be advisable to put in an IP network into a site to get SNMP traps out for alerts if a serial circuit with reduced attack surface is all that is needed for operations.

One issue with the ERC definition from the V5TAG transfer document is that of a BCA that only speaks non-routable protocols over a serial port. These BCAs do not use a routable protocol themselves and therefore can be considered to not have ERC because it is defined in terms of “routable protocol.” These BCAs, however, can have interactive user access using those serial connections. The SDT has kept ERC as-is with only conforming changes in order to not disrupt its scoping function as noted above. However, the IRA definition has been modified so that a device with only a serial, non-routable connection can now have IRA and be subject to CIP-005-8 Requirement R2; and, appropriate controls are now required for these IRA sessions without regard to ERC. The intention is to cover situations where a serial-only, non-routable BCA, such as a digital relay in a substation, has that serial communication converted to IP or other routable protocols thus providing IRA from users outside the substation to interact with the serial device. Such situations require the CIP-005-8 Requirement R2 protection.

In modifying both the IRA and Intermediate Systems definitions, the SDT moved related requirement language from the previous definition into CIP-005-8 Requirement R2. The SDT added the “…that originates from outside…” text to the high level Requirement R2, removing it from the IRA definition. In this case the language works in collaboration with the IRA definition to allow access to a system that originates and terminates inside the logical isolation from CIP-005-8 Requirement R1 Part 1.1 without requiring an Intermediate System. However, for remote access that originates from outside of the logical isolation that accesses a device inside of the Requirement R1 Part 1.1 isolation would require CIP-005-8 Requirement R2 protections.

Requirement language includes wording for required logical isolation containing either high or medium impact BCS or associated SCI to provide the equivalent logical protections for remote access that existed before. Existing ESPs under CIP-005-7 can be used to provide the “required logical isolation” and thus remain backward compatible.

Similarly, the applicability was updated for virtualized environments so that it applies for remote access to Management Modules, Management Systems and Management Interfaces that did not originate from within another of the entity’s instance of required logical isolation.

Requirement R2 Part 2.1:

Rationale

The Applicable Systems section of this requirement was updated to include SCI associated with high and medium impact BCS. This was done to ensure that same safeguards for remote access methods and technologies exist for the applicable SCI as for the high and medium impact BCS and associated PACS, EACMS, or PCA being hosted on that SCI. Backwards compatibility with CIP-005-7 is maintained for entities that do not currently use SCI.

The Applicable Systems section of this requirement was also updated to include Management Modules of SCI associated with high and medium impact BCS. This was done to ensure that same safeguards for remote access methods and technologies exist for the applicable SCI as for the high and medium impact BCS and associated PACS, EACMS, or PCA being hosted on that SCI. Backwards compatibility with CIP-005-7 is maintained for entities that do not currently use SCI.

The inclusion of the SCI is intended to target the Management Modules and Management Systems (included in SCI definition) of the associated SCI. This is to ensure that the management of the SCI being used to support BCS is also protected in an equivalent manner.

For Medium Impact BCS, the Applicable Systems wording was updated from "with ERC to "with IRA". This was done to cover serial connectivity associated IRA for those Applicable Systems without ERC. This aspect of IRA was missing from earlier versions of CIP-005. This change is intended to mitigate risks associated with a possible external (to the entity) attack vector in situations where serial connectivity is converted to network connectivity using a terminal server type device. This is one of the issues noted by the V5TAG and is not associated with changes required for virtualization. Please refer to the section of this document entitled "**External Routable Connectivity (ERC) and Interactive Remote Access (IRA)**."

The requirement language itself was simplified. Note the definitions of IRA and Intermediate System have been updated. Please note that the definition of IRA was changed to include serial communications connections. This change maintains backwards compatibility with CIP-005-7 except where serial connectivity is being used for IRA.

The required location of an Intermediate System was within the definition previously. The definition of Intermediate System has been simplified and the requirement to be logically isolated from its Applicable Systems is now within the requirement itself (Part 2.6.2) rather than within the definition.

Requirement R2 Part 2.2:

Rationale

The Applicable Systems was changed to Intermediate Systems from high or medium BCS and associated PCA. This change better reflects that this requirement is associated with the Intermediate System itself.

The requirement was changed from a specific technical based requirement for encryption to an objective based requirement to protect confidentiality and integrity of the IRA session. The proposed language of this requirement accounts for the possibility that other equally effective methods could be developed and deployed. This also prevents outdated encryption methods from being used that no longer meet the objective.

The changed requirement is backwards compatible with the CIP-005-7 except where outdated encryption methods have been used.

Requirement R2 Part 2.3:

Rationale

The Applicable Systems was changed to Intermediate Systems from high or medium BCS and associated PCAs. This change better reflects that this requirement is associated with the Intermediate System itself. Note that serial connection-based IRA is now included due to the IRA definition change. This change also clarifies where the requirement for multifactor authentication should be applied.

The changed requirement is backwards compatible with the CIP-005-7 except where serial connection-based IRA is being utilized.

Requirement R2 Part 2.4 – 2.5:

Rationale

The Applicable Systems section was changed to include SCI hosting High or Medium impact BCS or their associated PCA, including its Management Modules, in instances where vendor remote access is allowed to the SCI or Management Modules. The applicable systems were also modified such that only those with vendor remote access are in scope and thus need to have one or more methods for CIP-005-8 Requirement R2 Parts 2.4 and 2.5.

The inclusion of SCI is intended to target the Management Modules and Management Systems (included in SCI definition) of the associated SCI. This is to ensure that the management of the SCI being used to support BCS is also protected in an equivalent manner.

The requirements themselves have not been changed. Note that the requirement includes both vendor based IRA and system-to-system access.

Requirement R2 Part 2.6:

Rationale

This is a new requirement that applies to Intermediate Systems that are required by CIP-005-8 Requirement R2 Part 2.1. This is due to instances where Intermediate Systems have an externally accessible interface that may be used by external parties such as vendors or entity support staff using IRA across an internet connection to support a remote site. Since Intermediate Systems by nature provide IRA from a less-trusted network, a degree of separation from the higher-trust systems they are protecting is necessary in case the Intermediate System is compromised. Previously, this separation "requirement" was not an actual requirement but was contained within the glossary definition of Intermediate System ("…must not be located inside the ESP"). The SDT has removed this from the definition and included an objective in CIP-005-8 Requirement R2 Part 2.6.2 to permit only needed and controlled communications between the Intermediate System and the applicable systems it is providing IRA to.

In order to further mitigate the risk of a compromised virtualized Intermediate System hosted on SCI, Requirement CIP-005-8 Requirement R2 Part 2.6.1 restricts CPU and memory sharing on SCI to only its associated SCI itself and other Intermediate Systems.
In summary, CIP-005-8 Requirement R2 Part 2.6 is intended to mitigate the risk associated with "side channel" based attack vectors where it could be possible to compromise the Intermediate System from an external source and then subsequently access another VCA running on the same hypervisor within the SCI.

Requirement R3

Rationale

The Applicable Systems section of CIP-005-8 Requirement R3 was updated to include SCI hosting EACMS or PACS associated with high or medium impact BCS to ensure the same safeguards for vendor-initiated remote connections exist for the applicable SCI. Backwards compatibility with CIP-005-7 is maintained for entities that do not currently use SCI.

The Applicable Systems section of this requirement was also updated to include Management Modules of SCI hosting EACMS or PACS associated with high or medium impact BCS to ensure the same safeguards for vendor-initiated remote connections exist for the applicable Management Modules. Backwards compatibility with CIP-005-7 is maintained for entities that do not currently use SCI.

The inclusion of the SCI is intended to target the Management Modules and Management Systems (included in SCI definition) of the associated SCI to ensure the management of the SCI is also protected in an equivalent manner.

Former Background Section from Reliability Standard CIP-005-7

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BCS and require a minimum level of organizational, operational and procedural controls to mitigate risk to BCS.

Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BCS. For example, a single training program could meet the requirements for training personnel across multiple BCS.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.

- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

Technical Rationale for Reliability Standard CIP-005-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The ESP serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-

15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e. system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the “first line of defense within an Industry Control System (ICS) network environment”. The compromise of those devices that control access management could provide an outsider the “keys to the front door” of the ESP where BES Cyber Systems reside. An intruder holding the “keys to the front door” could use those “keys” to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[1].

NERC's final report on "*Cyber Security Supply Chain Risks*", states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks*" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

---

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an “Associated Protected Cyber Asset” of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually ‘command and control’ hosts on the Internet, or compromised ‘jump hosts’ within the Responsible Entity’s other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT’s intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity’s address space. The SDT’s intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and ‘deny by default’ type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear ‘perimeter type’ security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions (“TFEs”) rather than increased security.

As for dial-up connectivity, the Standard Drafting Team’s intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Physical Security of BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-006-7

January 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-006-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-006-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-006-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

Requirement R1 – Requirement R3

Rationale

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-006-7 for virtualization, SDT added SCI and matched it to the BCS already listed in Applicable Systems.

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-006-7 to align Physical Security of BES Cyber System (BCS) requirements with the virtualization changes. The conforming changes are as follows:

Applicable Systems containing High Impact BCS:

- Where the former Applicable Systems included High Impact BES Cyber Systems and their associated EACMS and PCA, the conforming change includes adding SCI to the applicability to match the existing High impact BCS and includes, "SCI hosting High Impact BCS or their associated EACMS or PCA." Affected Requirement Parts are:
    - Requirement R1 Part 1.3
    - Requirement R1 Part 1.4
    - Requirement R1 Part 1.5
    - Requirement R1 Part 1.8
    - Requirement R1 Part 1.9
    - Requirement R2 Part 2.1
    - Requirement R2 Part 2.2
    - Requirement R2 Part 2.3

Applicable Systems containing a variant of Medium Impact BCS:

- Where the former Applicable Systems included Medium Impact BES Cyber Systems without ERC, the conforming change is adding "SCI hosting..." Affected Requirement Part is:
    - Requirement R1 Part 1.1

- Where the former Applicable Systems included Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS and PCA, the conforming change is adding SCI to the applicability to match the updated Medium impact BCS and includes, "SCI, with ERC, hosting Medium Impact BCS or their associated EACMS or PCA." Affected Requirement Parts are:
    - Requirement R1 Part 1.2
    - Requirement R1 Part 1.4
    - Requirement R1 Part 1.5
    - Requirement R1 Part 1.8
    - Requirement R1 Part 1.9
    - Requirement R2 Part 2.1
    - Requirement R2 Part 2.2
    - Requirement R2 Part 2.3

Applicable Systems containing a variant of Physical Access Control Systems (PACS):

- Where the former Applicable Systems included Physical Access Control Systems (PACS) associated with High Impact BES Cyber Systems, the SDT added SCI to match the existing BCS by including "SCI hosting High Impact BCS"; Here, the SDT also extended SCI hosting applicability to the High Impact BCS's associated EACMS or PCA. CIP-006-7 contains several Requirement Parts where the target of the control includes the PACS themselves. In this case, the SDT determined the appropriate PACS to protect would be those that secure the Applicable Systems of Requirement R1 Parts 1.2 & 1.3. The SDT is constrained by the current SAR to only apply these updates to the virtualized versions of those targets, which resulted in the various "SCI hosting…" bullets included under PACS, as well as the SCI hosting PACS references within the applicability of these requirements." Lastly, the SDT added a separate entry for "SCI hosting PACS associated with High Impact BCS"
    - Requirement R1 Part 1.1
    - Requirement R1 Part 1.6
    - Requirement R1 Part 1.7
    - Requirement R3 Part 3.1

- Where the former Applicable Systems included Physical Access Control Systems (PACS) associated with Medium Impact BES Cyber Systems with ERC, the SDT added SCI to match the existing BCS by including "SCI hosting High Impact BCS"; Here, the SDT also extended SCI hosting applicability to the associated EACMS or PCA of the Medium impact BCS with ERC. CIP-006-7 contains several Requirement Parts where the target of the control includes the PACS themselves. In this case, the SDT determined the appropriate PACS to protect would be those that secure the Applicable Systems of Requirement R1 Parts 1.2 & 1.3. The SDT is constrained by the current SAR to only apply these updates to the virtualized versions of those targets, which resulted in the various "SCI hosting…" bullets included under PACS, as well as the SCI hosting PACS references within the applicability of these requirements." Lastly, the SDT added a separate entry for "SCI hosting PACs associated with Medium Impact BCS with ERC".
    - Requirement R1 Part 1.1
    - Requirement R1 Part 1.6
    - Requirement R1 Part 1.7
    - Requirement R3 Part 3.1

Applicable Systems containing Locally mounted hardware or devices at the Physical Security Perimeter (PSP):

- Where the former Applicable Systems included locally mounted hardware with associated with High Impact BES Cyber Systems, the SDT added SCI to match the existing BCS by including "SCI hosting PACS associated with High Impact BCS". Affected Requirement Part is:
    - Requirement R3 Part 3.1
- Where the former Applicable Systems included locally mounted hardware associated with Medium Impact BES Cyber Systems with External Routable Connectivity, "the SDT added SCI to match the existing BCS by including "SCI hosting PACs associated with Medium Impact BCS with ERC." Affected Requirement Part is:
    - Requirement R3 Part 3.1

Other modifications:

- The SDT also evaluated where CIP Exceptional Circumstances (CEC) should be included, and has added this provision to the following requirement parts:
    - Requirement R1 Part 1.8.

      Rationale: Responsible Entities may not be able to log entry of each individual with authorized unescorted physical access into each Physical Security Perimeter if a facility that contains the Physical Security Perimeter or Physical Access Control System is damaged or destroyed.
    - Requirement R1 Part 1.9.

      Rationale: Responsible Entities may not be able to retain access logs of entry of individuals into each Physical Security Perimeter if a facility that contains the Physical Security Perimeter or Physical Access Control System is damaged or destroyed.
    - Requirement R2.

      Rationale: Responsible Entities may not be able to implement the documented visitor control program during certain conditions that qualify as CIP Exceptional Circumstances. Conditions could include a risk of injury or death, a natural disaster that damages or destroys a Responsible Entity's facilities, or first responders the require access to the Physical Security Perimeter.
- The SDT chose to remove the reliance on a Technical Feasibility in favor of the updated term “per system capability.”
    - Requirement R1 Part 1.3.

      Rationale: The SDT contends that the term still requires an entity to document the limit to the system’s capability with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception.
- The SDT deleted Requirement R1 Part 1.10 from CIP-006-7 because it is incorporated into CIP-005-8 Requirement R1 Part 1.3.

Former Background Section from Reliability Standard CIP-006-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-006-6

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-006-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed “six-wall” boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

- Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the “guard” has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an "an equally effective logical protection" in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity's BES Cyber Systems while not requiring controls to be implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — System Security Management

Technical Rationale and Justification for Reliability Standard CIP-007-7

January 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-007-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-007-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-007-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." Document for reference when reading the technical rationale that follows.

General Considerations

Requirement R1

General Considerations for Requirement R1

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-007-7 for virtualization, the SDT added SCI and matched it to the BCS and associated Cyber Assets already listed in Applicable Systems. This approach keeps the SCI applicability parallel to each existing variant of medium impact BCS (i.e. Medium impact BCS vs. Medium impact BCS with External Routable Connectivity (ERC) vs. Medium impact BCS at Control Centers etc.)

Change Rationale Requirement R1:

The SDT has changed the name of the Requirement R1 table to “System Hardening” to more clearly reflect the security objective of the entries in the table which is to harden the applicable systems through limiting access to logical services and physical ports.

Change Rationale Requirement R1 Part 1.1:

Requirement R1 Part 1.1 changes to focus on network accessible services rather than port numbers. The ability to refer to ports is retained for compatibility. In virtualized environments, services are used in the underlay and the SDT is avoiding requiring tracking functionality in the underlay at a port level versus the service level. As services can be configured to use any logical port number, the focus shifts to what services (SSH, web server, etc.) are enabled rather than a port number. If services cannot be determined, such as an open port showing on a firmware based device, then documenting the need for port numbers (or ranges) is also still supported.

The SDT made the decision to not include SCI in Part 1.1 and to create a separate requirement for SCI and associated Management Modules in Requirement R1 Part 1.3. The difference between these two requirement parts is Part 1.1 concentrates on all network accessible services, while Part 1.3 is scoped to all services used by the SCI or its Management Modules (whether network accessible or not) as SCI presents a higher risk.

The SDT chose to remove the reliance on a Technical Feasibility Exception in favor of the updated term “per system capability.” The SDT contends that the term still requires an entity to document the limit to the system’s capability with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception.

Change Rationale Requirement R1 Part 1.2:

The SDT chose to include “SCI hosting…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be in scope of this requirement part.

The SDT also chose to consolidate the non-programmable components in the Applicable Systems into one statement that conforms to the broader logical isolation concepts instead of limiting to the former perimeter model alone.

Change Rationale Requirement R1 Part 1.3:

Requirement R1 Part 1.3 is a new requirement intended to apply security and hardening to SCI by enabling only needed services. In order to maintain backwards compatibility, the SDT purposely wrote the requirement to exclude devices not used in a virtualized environment, which remain covered under Requirement R1 Part 1.1.

The SDT made the decision to create a separate requirement for SCI and associated Management Modules in Requirement R1 Part 1.3, which is scoped to all services used by the SCI or its Management Modules (whether network accessible or not, as in Requirement R1 Part 1.1) as SCI presents a higher risk.

“Per system capability” was used with the intent of allowing Responsible Entities to make use of systems that are Applicable Systems, but are unable to disable certain services.

Requirement R2

Change Rationale Requirement R2:

The SDT made conforming changes where necessary with Requirement R2 to remove reliance on the Cyber Asset term, choosing to reference the system instead as SCI and Management Modules are included in the Applicable Systems column.

The SDT chose to include “SCI hosting…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in applicable BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACS, PACS, or PCAs, and should therefore be in scope of this requirement part.

The SDT also chose to include Management Modules of SCI in the Applicable Systems column to ensure they also received applicable security patching.

Backward Compatibility

CIP-007-7 Requirement R2 retains backward compatibility for entities without installed SCI.

The SDT intends that entities take full advantage of their virtualization infrastructure in order to ease the overhead associated with patch management. While many of the entity’s existing processes will remain the same, (such as those associated with tracking the source of security patches, evaluation of the applicability of available patches and mitigation plans for those applicable patches that cannot be installed) new or modified processes around the installation of patches can be used (for example, parent images, remediation VLANs, etc.)

Parent Images

One of the interesting nuances of virtualization is the concept of parent/child relationships.

Some VCAs utilize a “parent image” type methodology where the specific VCA software and operating system is merely a child instance of a parent image. In such cases, the application of security patches to the parent image also applies the same changes to any children of that image. As there may be many child instances, the administrative overhead associated with patching of those instances can be greatly reduced.

Dormant Instances

There are times when VCAs are not being used and are idle. Physical instances of the assets are always left up and running in order to receive applicable patches, software updates, configuration updates, etc.

Leveraging the built in virtualization features allows idle resources to be reassigned to tasks at hand without incurring additional overhead of tracking which dormant virtual instances require patching. Dormant virtual instances are merely just files with the saved state of the VCA. Dormant instances are not VCAs themselves nor Applicable Systems until they become active instances again.

Where a dormant virtual instance is also the child instance of a parent image, the application of security patches to the parent image will also make the same changes automatically when needed to any out of date dormant child virtual instances when they are restarted.

In most cases, a dormant virtual child instance is made active again on a remediation type network where any missing security patches (compared to the parent image) are automatically applied before it is placed back into active service.

Saved Images

Similar to dormant child images, saved child images or snapshots may be also used as functional backups for CIP-009 purposes in order to provide fast restoration and better availability. If an active VCA becomes corrupted, a saved image can be made active where the application of any missing security patches (compared to the parent image) will be automatically applied before being placed back into active service.

Self-Contained Applications

Self-Contained Applications (SCA) are treated similar to traditional installed application software, and patched as a unit.

Change Rationale Requirement R2 Parts 2.1-2.4:

The SDT has updated the applicable systems to include SCI and Management Module and made conforming changes with the requirement parts and measures.

Requirement R3

Change Rationale Requirement R3:

The SDT chose to modify the name of the Table in R3 from Malicious Code Prevention to the term used by the National Institute of Standards & Technology (NIST), Malicious Code Protection, as that more accurately clarifies the security objective of protecting BCS from malicious code.

The SDT chose to include "SCI hosting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in applicable BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BES Cyber Systems, EACMS, PACS, or PCAs, and should therefore be in scope of this requirement part.

Change Rationale Requirement R3 Parts 3.1-3.3:

The SDT has updated the applicable systems to include SCI and Management Modules.

Requirement R4

Change Rationale Requirement R4:

Change Rationale Requirement R4 Part 4.1:

The SDT chose to include "SCI hosting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in applicable BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be in scope of this requirement part.

The SDT determined the entire structure of the "at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)" language could be simplified to "per system capability" since the Applicable Systems column clarifies what systems are included.

Additionally, the SDT chose to insert the word "security" as a clarifier to which events are to be logged.

Change Rationale Requirement R4 Part 4.2:

The SDT chose to include "SCI hosting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in applicable BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be in scope of this requirement part.

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the "Cyber Asset" term, as well as the ambiguity that would have existed if the term "BES Cyber System" were left in place while the Applicability Column included SCI.

Change Rationale Requirement R4 Part 4.3:

The SDT chose to include "SCI hosting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in applicable BES Cyber Systems, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be in scope of this requirement part.

The SDT also chose to remove the reliance on a Technical Feasibility from Part 4.3 in favor of the updated term "per system capability." The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception.

Change Rationale Requirement R4 Part 4.4:

The SDT chose to include "SCI hosting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in applicable BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be in scope of this requirement part.

Requirement R5

Change Rationale Requirement R5:

Change Rationale Requirement R5 Parts 5.1 – 5.7:

The SDT chose to include "SCI hosting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in applicable BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be in scope of this requirement part.

Change Rationale Requirement R5 Parts 5.1, and 5.6 – 5.7:

The SDT chose to remove the reliance on "Technical Feasibility" in favor of the updated term "per system capability." The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception.

Former Background Section from Reliability Standard CIP-007-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-007-6

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-007-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible (“listening”) ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset’s function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed ‘needed.’

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

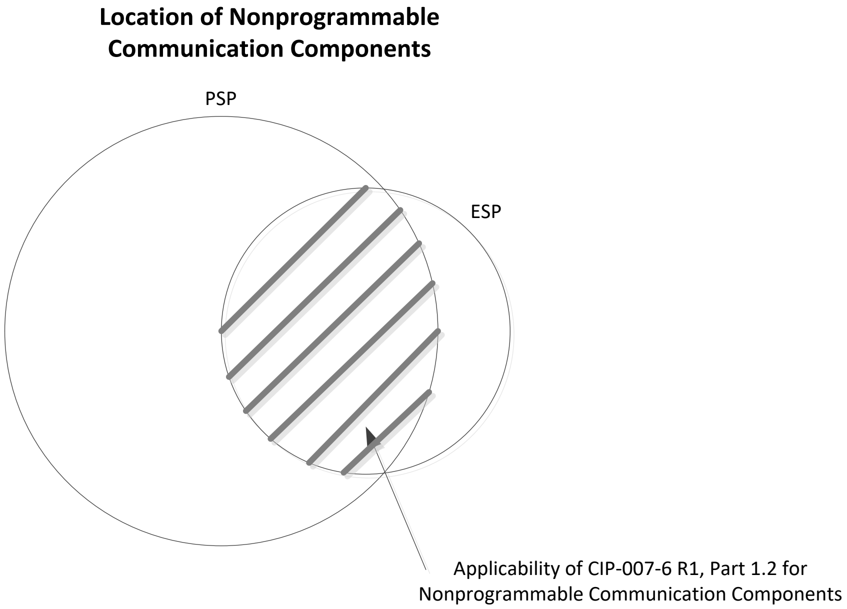
The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:



Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media (“transient devices”) in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms

- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security – Incident Reporting and Response Planning

Technical Rationale and Justification for Reliability Standard CIP-008-7

January 2021

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-008-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-008-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

Requirement R1 – Requirement R4

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-008-6 to align incident reporting and response planning requirements with the virtualization changes.

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-008-7 for virtualization, the SDT added SCI hosting High or Medium Impact BCS or their associated EACMS to each of the Parts in Applicable Systems for Requirement R1 – Requirement R4.

Former Background Section from Reliability Standard CIP-008-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

Medium Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

Technical Rationale for Reliability Standard CIP-008-6

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-6. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-008-6 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 19, 2018, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 848. In this Order FERC directed the North American Electric Reliability Corporation (NERC) to "develop and submit modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access and Control or Monitoring System (EACMS)." (Order 848, Paragraph 1)

In response to the directive in Order No. 848, the Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require Responsible Entities to implement methods augmenting the mandatory reporting of Cyber Security Incidents to include: "(1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report included specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT)." (Order 848, Paragraph 3)[1]

New and Modified Terms Used in NERC Reliability Standards

CIP-006-6 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms:

Cyber Security Incident

A malicious act or suspicious event that:

- *For a high or medium impact BES Cyber System, compromises, or attempts to compromise the, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or*
- *Disrupts, or attempts to disrupt, the operation of a BES Cyber System.*

In response to FERC Order 848, Paragraph 1, the SDT modified the Cyber Security Incident definition to include Electronic Access Control or Monitoring Systems (EACMS) associated with high or medium impact BES Cyber Systems, in response to the Order.

---

[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

The addition of high and medium impact BES Cyber Systems considers the potential unintended consequences with the use of the existing definition in CIP-003-7. It also provides clarity that only low impact BES Cyber Systems are included within the definition. ESP or EACMs that may be defined by an entity for low impact BES Cyber Systems are not part of the definition.

An attempt to disrupt the operation of a BES Cyber System is meant to include, among other things, a compromise of a single BES Cyber Asset within a BES Cyber System. For example, malware discovered on a BES Cyber Asset is an attempt to disrupt the operation of that BES Cyber System.

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:

- *A BES Cyber System that performs one or more reliability tasks of a functional entity;*
- *An Electronic Security Perimeter of a high or medium impact BES Cyber System; or*
- *An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber Systems.*

The Reportable Cyber Security Incident definition was modified to comply with FERC Order 848. In response to Paragraph 54 of the Order, the SDT modified the definition to include incidents that compromised or disrupted an ESP or an EACMS. The team also added the qualifying clause for “A BES Cyber System that performs one or more reliability tasks of a functional entity” to clarify what was compromised or disrupted, thus not extending the scope to Protected Cyber Assets (PCAs). In response to comments, the SDT left the entire definition of BES Cyber system in Reportable Cyber Security Incident to provide clarity.

It is also important to understand the relationship between the two definitions, the requirement language, and how they work in concert to classify events and conditions at varied levels of significance as the Registered Entity executes its process and applies its defined criteria to determine if reporting is required.

Electronic Access Control or Monitoring Systems (EACMS)

The drafting team spent significant time discussing this topic among its members, through industry outreach, and with FERC staff. The team believes by not specifically referencing the five functions in Order 848, we have reduced complexity and made compliance with the Standard achievable. The drafting team asserts that the five functions are equivalent to the current definition of EACMS in the NERC Glossary of Terms. If entities have questions about application of the EACMS definition, the drafting team advises entities to discuss those questions directly with NERC.

Requirements R1, R2, and R3

General Considerations for Requirement R1, Requirement R2, and Requirement R3

FERC Order 848, Paragraph 1, directs modifications to Reliability Standards to require reporting of incidents that compromise, or attempt to compromise a responsible entity's ESP or associated EACMS. The intent of the SDT was to minimize the changes within CIP-008 and address the required modifications. To do this, the SDT added "and their associated EACMS" to the "Applicable Systems" column for Requirements R1, R2, and R3.

To add clarity to "attempts to compromise," the drafting team created Part 1.2.1 to require entities to establish and document their process to include criteria to evaluate and define attempts to compromise. This requirement maps to Requirement 4 Part 4.2, which requires entities to use that entity-defined process for determining which incidents entities must report.

The use of the language describing Cyber Security Incident(s) as being "an attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the 'Applicable Systems'" column for the Part is meant to clarify which Cyber Assets are in scope for attempts to compromise reporting by entities. This language is used throughout the standard.

Moving Parts of Requirement R1 to Requirement R4

To minimize the changes to Requirement R1, the SDT created Requirement R4 and consolidated all the CIP-008-6 reporting requirements. The SDT deleted Requirement R1 Part 1.2 reporting requirements from CIP-008-5, and moved them to Requirement R4 for this purpose.

Inclusion of "Successor Organizations" throughout the Requirement Parts

The SDT recognizes that organizations are constantly evolving to meet emerging needs, and may re-organize or change their names over time. The ICS-CERT has completed its name change to the National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems. The E-ISAC previously re-branded its name and may again in the future. By following Requirement R4 references to E-ISAC and NCCIC with "or their successors" the SDT is ensuring that Requirement R4 can be implemented even if the names of E-ISAC and NCCIC change or a different agency takes over their current roles.

Requirement R4

General Considerations for Requirement R4

Requirement R4 is a new requirement focused on mandatory reporting of Reportable Cyber Security Incidents and includes attempts to compromise systems in the "Applicable Systems" column. Previously, CIP-008-5 defined reporting requirements for Reportable Cyber Security Requirements (Requirement R1 Part 1.2) only.

Required Reportable Incident Attributes

Requirement R4.1 specifies that initial notifications and updates must include three attributes: 1) functional impact, 2) attack vector used, and 3) level of intrusion achieved or attempted. These attributes are taken directly from the Order. (FERC Order No. 848, paragraph 89).

The SDT understands that some or all of these attributes may be unknown at time of initial notification. To account for this scenario the SDT included "to the extent known" in the requirement language. There is an expectation that update reporting will be done as new information is determined or unknown attributes become known by the entity. There could be cases, due to operational need, that all the attributes may never be known, if this case presents itself that information should be reported.

Methods for Submitting Notifications

Requirement R4 Part 4.2 allows responsible entities to submit notification using any method supported by E-ISAC and NCCIC. The SDT did not prescribe a particular reporting method or format to allow responsible entities' personnel to focus on incident response itself and not the method or format of reporting. It is important to note the report must contain the three attributes required in Requirement R4 Part 4.1 as they are known, regardless of reporting method or format.

Notification Timing

Requirement R4 Part 4.2 specifies two timelines for initial notification submission; one hour for Reportable Cyber Security Incidents; and end of next calendar day for attempts to compromise systems in the "Applicable Systems" column. Paragraph 3 of FERC Order No 848 directly states that reporting deadlines must be established. Paragraph 89 further states that "timelines that are commensurate with the adverse impact to the BES that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES."

- *Reportable Cyber Security Incidents* – The SDT wrote Requirement R4 Part R4.2 to use a one hour deadline for reporting of these events because incidents in this category include successful compromise of ESP(s), EACMS, or BES Cyber System(s). One hour is referenced directly in FERC Order No 848 paragraph 89 and is also the current reporting requirement in CIP-008-5.
- *Cyber Security Incident that was an attempt to compromise one or more systems identified in the "Applicable Systems" column* - Due to the lower severity of these unsuccessful attempts at compromising ESP(s), EACMS, or BES Cyber System(s), the SDT proposed a longer reporting timeframe. The intent behind the decision to add "By the end of the next calendar day" (11:59 pm local time) was to give responsible entities additional time to gather facts prior to notifications for the less severe attempts to compromise Applicable Systems. It is important to note that compliance timing begins with the entity's determination that attempt to compromise meets the process they defined in Requirement R1 Part 1.2.1.

The SDT understands initial notification may not have all the details when first submitted. It is expected, however, that information that has been determined is reported within the notification deadlines. Additionally, it is important to note the wording in Requirement R4 Part 4.2. The "compliance clock" for the report timing begins when the Responsible Entity executes its process from Requirement R1 Part 1.2.1 and a determination has been made that the type of incident which has occurred qualifies as reportable.

Technical rationale taken from the Guidelines and Technical Basis (GTB) CIP-008-5 Requirement 1 provides additional justification for the SDT to maintain the one hour timeframe for Reportable Cyber Security Incidents.

> *"The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."*

In 2007, the Electricity Information Sharing and Analysis Center (E-ISAC) was known as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Its voluntary procedures required the reporting of a cyber-incident within one hour of an incident. CIP-008-1 required entities to report to the ES-ISAC.

In FERC Order No. 706[2] (July 18, 2008), the Commission concluded that the one-hour reporting limit was reasonable [P 663]. The Commission further stated that it was leaving the details to NERC, but it wanted the reporting timeframe to run from the "**discovery**" of the incident by the entity, and not the actual **"occurrence"** of the incident [P 664].

CIP-008-2 and CIP-008-3 were silent regarding the required timeframe for reporting, but it was specifically addressed in CIP-008-5. In the October 26, 2012, redlined version of CIP-008-5, the proposed language for initial notification originally specified "one hour from **identification**" of an incident. This aligned with the Commission's decision in Order No. 706, for the clock to start with the discovery of an incident. However, the Standard Drafting Team changed "one hour from identification" to "one hour from the **determination** of a Reportable Cyber Security Incident". This language was subsequently approved and incorporated into CIP-008-5.

These changes, from "occurrence" to "discovery" to "determination," provide the additional time needed for the entity to apply its specifically created process(es) for determining whether a Cyber Security Incident rises to the level of required reporting. This determination timeframe may include a preliminary investigation of the incident which will provide useful information to other entities to help defend against similar attacks.

---

[2] 2008, Federal Energy Regulatory Commission, Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706.

Notification Updates

Requirement R4 Part 4.3 requires that Responsible Entities submit updates for the required attributes upon determination of new or changed attribute information, if any. The SDT added this language to provide entities sufficient time to determine attribute information, which may be unknown at the time of initial notification, and which may change as more information is gathered. The intent of Requirement R4 Part 4.3 is to provide a method for Responsible Entities to report new information over time as their investigations progress. NOTE: The SDT does not intend updates specified in Requirement R4. Part 4.3 to expose responsible entities to potential violations if, for example, initial and updated notification on the same attribute have different information. This is expected since knowledge of attributes may change as investigations proceed. Rather, the intent of Requirement R4 Part 4.3 is to have a mechanism to report incident information to E-ISAC and NCCIC (and thereby industry) upon determination of each required attribute.

The intent is that the entity report what is known and document the reason not all attributes could become known and ultimately be reported in conditions where, e.g. a Cyber Asset was restored completely, removing all forensic evidence in order to restore operations, which caused the entity to conclude its investigation without having a complete knowledge of the three required attributes.

The SDT asserts that nothing included in the new reporting Requirement R4, precludes the entity from continuing to provide any voluntary sharing they may already be conducting today.

Technical Rationale for Reliability Standard CIP-008-5

This section contains the Guidelines and Technical basis as a "cut and paste" from CIP-008-5 standard to preserve any historical references.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for Reportable Cyber Security Incidents.

Entities may use an actual response to a Reportable Cyber Security Incident as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise.

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for Reportable Cyber Security Incidents. There are several examples of specific types of evidence listed in the measure.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

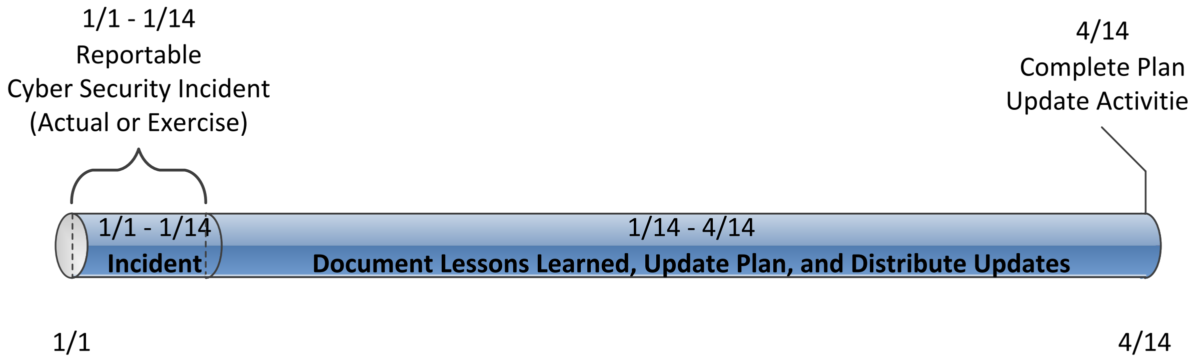
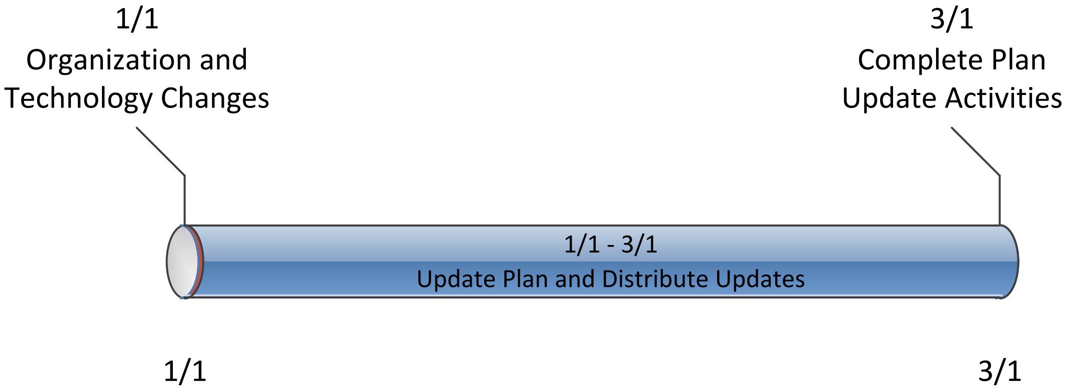


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals.

Figure 2: Timeline for Plan Changes in 3.2



Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)
"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)
Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)
Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)
Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)
Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)
Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)
Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Recovery Plans for BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-009-7

January 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-009-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-009-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-009-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

Requirement R1 – Requirement R3

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-009-7 to align recovery planning requirements with the virtualization changes.

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-009-7 for virtualization, the SDT added SCI and matched it to the BCS already listed in Applicable Systems. The conforming changes are as follows:

- Where the former Applicable Systems listed High and Medium Impact BCS and their associated EACMS or PACS, the conforming change is "SCI hosting High or Medium Impact BCS or their associated EACMS or PACS". Affected Requirement Parts are:
    - Requirement R1 Part 1.1
    - Requirement R1 Part 1.2
    - Requirement R1 Part 1.3
    - Requirement R1 Part 1.5
- Where the former Applicable Systems was limited to High Impact BES Cyber Systems, the conforming change adds only "their associated SCI". Affected Requirement Parts are:
    - Requirement R2 Part 2.3
- Where the former Applicable Systems listed scoped the Medium Impact BCS aspect to those at Control Centers only, the conforming change is "SCI hosting High or Medium Impact BCS at Control Centers or their associated EACMS or PACS". Affected Requirement Parts are:
    - Requirement R1 Part 1.4
    - Requirement R1 Part 2.1
    - Requirement R2 Part 2.2
    - Requirement R3 Part 3.1
    - Requirement R3 Part 3.2

Additionally, the use of the term BES Cyber System has been replaced with applicable system within the requirement language to align the requirement with the applicability for each Requirement Part.

Former Background Section from Reliability Standard CIP-009-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.

An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-009-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-009-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, “A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures.”

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, “[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and ‘boots on the ground’ response (e.g., firefighters decontaminating mock victims).”

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

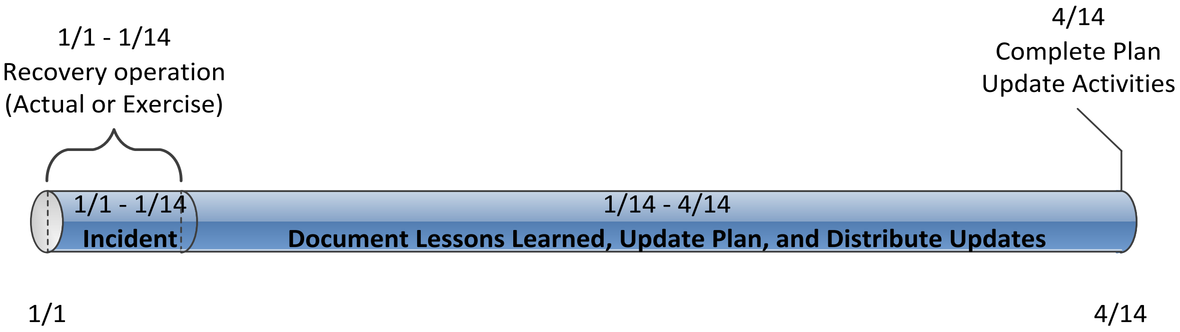


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

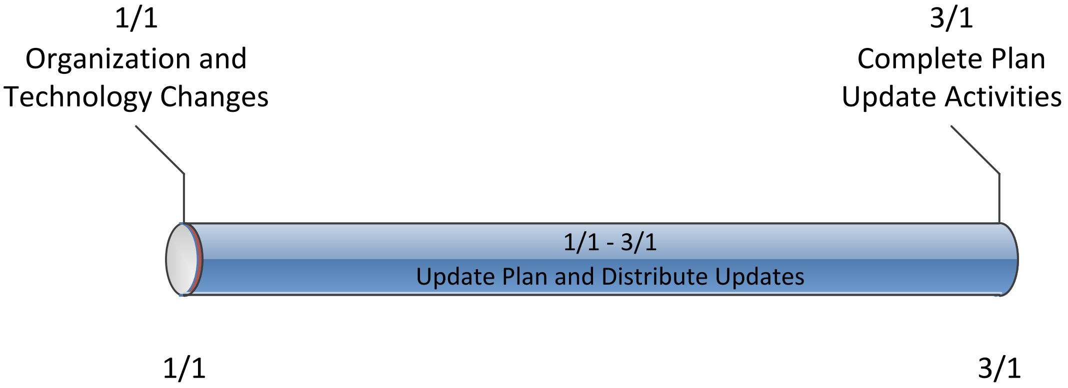


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-5

January 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-010-5

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-5. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-010-5 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

The proposed changes in CIP-010-5 from the Project 2016-02 SDT concern the use of several facets of virtualization technologies. Virtualization allows for such technologies as new logical isolation controls for Shared Cyber Infrastructure (SCI), remediation VLANs, parent/child images, dormant virtual machines (VMs), and Self-Contained Applications (SCA), (i.e. containers). Enabling and clarifying the use of these technologies is the basis of the proposed changes in CIP-010-5. A general introduction to each of these technologies follows.

Shared Cyber Infrastructure (SCI)

Virtualization abstracts the software layers (the OS and applications) from the underlying hardware to allow for hardware to be shared among several Virtual Cyber Assets (VCAs). Hypervisors include security controls to keep these workloads logically isolated from one another and their requirements are within other CIP standards such as CIP-005. However, with any type of shared infrastructure, the need for change management requirements is elevated for those security controls that allow for the 'shared' in SCI. Such controls are added to the change management requirements in CIP-010-5.

Remediation VLAN

Remediation VLAN is a term used to describe a logical network segment in which a computing device can be isolated from other production systems and examined to ensure the integrity and validity of the configuration and software installed on the device before it is permitted to transition to the production network segment.

This examination is policy driven meaning that the administrator is able to configure what the minimum requirements are for admission to the production network. Examples of this might be minimum operating system patch levels or recent anti-virus definitions.

If during the examination of the computing device, it is found to not comply with the requirements defined in the policy, an administrator may intervene to manually remediate the deficiencies, or the system which was used to examine the device may communicate the deficiencies to the device with instructions on how to remediate itself in an automated fashion. After the remediation actions are taken, the computing device can request to be re-examined and if the requirements dictated by the policy are now met, it will be permitted access to the production network segment.

Parent/Child Images

When a VCA is ‘powered on’, it instantiates (“boots”) from a disk image file. Since the boot ‘disk’ is a file and not hardware, many individual VCA’s can use the same “parent” image as the basis for their own “child” image. This allows for example patching of an OS to occur to a parent image and the child images then pick up that patched image upon their next instantiation.

Dormant VMs

A VCA that is not instantiated (i.e. not ‘booted up’ and executing) is a dormant VM. It exists not as a traditional cyber asset, but simply as a file. VCA’s can be created for specialized purposes such as to run troubleshooting tools and only be instantiated when needed with long periods of times in between during which they exist as a file. They are not up and running and on the network where they are managed and patched on a regular basis. However, these can go hand in hand with remediation VLANs which would bring them up to date as soon as they do instantiate but before they have access to any other systems.

Self-Contained Applications (SCA)

An SCA or “container” is an application or function that is packaged to be as self-sufficient as possible to enable increased portability across environments. An SCA doesn’t depend on its software dependencies to be pre-installed on the particular server it is running on at the moment. This also allows for sandboxing applications from each other that may require different versions of the same software libraries. The point of SCAs are to abstract as much as possible from any underlying OS dependencies so they can be extremely portable.

General Considerations

SCI is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-010-5 for virtualization, the SDT evaluated the existing Applicable Systems and added hosting SCI (and in some case Management Modules of SCI) matched to each applicable BCS variant and associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), or (Protected Cyber Assets (PCAs) already listed in Applicable Systems. This approach keeps the SCI and Management Module applicability parallel to each existing variant of medium impact BCS (i.e. Medium Impact BCS vs. Medium Impact BCS with External Routable Connectivity (ERC) vs. Medium Impact BCS at Control Centers etc.).

Requirement R1

General Considerations for Requirement R1

In prior versions, CIP-010 Requirement R1 has required developing a baseline configuration that consisted of five (5) items (OS, installed and custom software, patches, ports). The baseline configuration was then used in the remainder of Requirement R1 and R2 as the basis of change management including testing. At a high level, the current Requirement Part 1.1 was to develop a baseline config, Requirement R1 Part 1.2 was to authorize and document changes to the items in the baseline config, and Requirement R1 Part 1.3 was to update the baseline config within a specific timeframe of a change. This tended to focus the requirement on documenting past changes.

In CIP-010-5, as the SDT considered the more policy-based and automated virtualization technologies discussed in the previous section, the SDT determined to change the focus of Requirement R1 towards a security objective of authorizing upcoming changes rather than maintaining a baseline configuration. Maintaining baseline configurations remains one possible "how", but it is no longer the only prescribed "how." The phrase "baseline configuration" has been removed from CIP-010-5 as a result. This maintains compatibility with current state but allows flexibility for virtualization technologies. This also ensures the focus is not on documenting past changes but the authorization of current or future changes, thus making the requirement forward looking with a clearer security objective.

Rationale for Requirement R1 Part 1.1

The original CIP-010 Requirement R1 Part 1.1 included establishing a baseline configuration for assets that included a set of items that would then be monitored for changes in the remaining parts of Requirement R1. This process is continued in the replacement for Requirement R1 and its Parts, however the documentation requirement (CIP-010-4 Requirement R1 Part 1.1) is no longer focused on a documentation only activity. While a Responsible Entity can benefit from documenting the configuration or the various elements of Requirement R1 Part 1.1 (1.1.1 – 1.1.6) this is no longer a requirement on its own. Maintaining this documentation is now one possible control to use to ensure changes to those elements are managed as required.

Additional changes were introduced to allow for or enable further use of virtualization. Specifically, the addition of "images used to derive operating systems or firmware" found in Requirement Part 1.1.1 is accounting for the concept of virtualized systems based on a "parent image." These images may be updated separately from a derived virtual machine, and become active as soon as the virtual machine is rebooted. In this case, changes to this parent image must follow the management requirements found in Requirement R1.

SCA are called out specifically in Requirement R1 Parts 1.1.2 and 1.1.3 to ensure that changes to these applications are authorized as well. These "containers" are usually replaced (not patched) from a repository and changes to the SCAs in the repository should be authorized since instances of the SCA typically automatically update from the repository.

Specific configuration items are included which apply only to SCI. These exist because the SDT determined that SCI that hosts BCS or associated EACMS, PACS or PCAs have controls that apply to specific configuration items relevant only to SCI.

Requirement R1 Part 1.1.4 has been changed to focus more on services than port numbers, although both are allowed.

Requirement R1 Part 1.1.5 was modified to remove the unnecessary “Any”.

Requirement R1 Part 1.1.6 is a new addition in order to require the authorization of changes to SCI configuration as it pertains to other required security controls (such as in CIP-005). The sharing of infrastructure puts a premium on the management of the security controls that enforce the logical isolation between tenants and the services the SCI itself uses. These areas that should fall under a CIP-010 management program are contained in Requirement R1 Part 1.1.6.

The SDT chose to include “SCI hosting…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset’s supporting hardware’s impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be the focus of Requirement R1 Part 1.1.

Rationale for Requirement R1 Part 1.2

The SDT chose to include “SCI hosting…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset’s supporting hardware’s impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be the focus of Requirement R1 Part 1.2.

The addition of “For each change *to the items listed in Part 1.1*” is used to scope the changes to only those listed in Requirement R1 Part 1.1, as a replacement to “deviations from the existing baseline configuration”, of applicable systems.

The addition of CIP Exceptional Circumstances (CEC) to Requirement R1 Part 1.2.1 was made because verification and documentation of cyber security controls prior to emergency change could impede Responsible Entities' efforts to recover from events or conditions that qualify as CEC.

Rationale for Requirement R1 Part 1.3

The addition of “For each change *to the items listed in Part 1.1*” is used to scope the changes to only those listed in Requirement R1 Part 1.1, as a replacement to “deviations from the existing baseline configuration”, of applicable systems.

The SDT chose to remove the reliance on a “Technical Feasibility Exception” in favor of the updated term “per system capability.” The SDT contends that the term still requires an entity to document the limit to the system’s capability with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception (TFE).

Additionally, the SDT chose to add to the phrase "that minimizes adverse effects" with "and differences with the production environment" to eliminate the dependency on baseline configuration. The SDT also enabled CIP-010-5 for the use of Remediation VLANs for testing. This Remediation VLAN is not be considered a part of the production BCS environment and could help facilitate a secure means of testing prior to implementing the change in the production BCS environment.

The addition of CEC to Requirement R1 Part 1.3.1 was made because testing in a test environment and documenting test results may impede Responsible Entities' efforts to recover from events or conditions that qualify as CEC.

Rationale for Requirement R1 Part 1.4

The SDT chose to include "SCI hosting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in BCS. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset's supporting hardware's impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS and should therefore be the focus of Requirement R1 Part 1.4.

The removal of "deviations from the existing baseline configuration" is a conforming change, with direct references to the specific Requirement R1 Part 1.1, sub-parts 1.1.1, 1.1.2, and 1.1.5.

Requirement R2

General Considerations for Requirement R2

The SDT has added the term "unauthorized" into Requirement R2 Part 2.1 to focus it on the risk of unauthorized changes. Many implementations will perform this task by monitoring all changes and looking for unauthorized changes within that population. However, if a way to filter out authorized changes can be implemented and an entity is able then to monitor just unauthorized changes that should fulfill the requirement.

Requirement R3

General Considerations for Requirement R3

The SDT chose to include "SCI hosting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset's supporting hardware's impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be a target of this requirement part itself.

Rationale for Requirement R3 Part 3.1

Conforming changes only to Applicable Systems (see General Considerations for Requirement R3 above).

Rationale for Requirement R3 Part 3.2

The SDT chose to remove the reliance on a "Technical Feasibility Exception" in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's

capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

In Requirement R3 Part 3.2.1, conforming changes have been made to remove the baseline configuration dependency.

Rationale for Requirement R3 Part 3.3

The requirement part has been rewritten to explicitly allow the use of remediation VLANs to perform the vulnerability assessment and remediation activities while the system is located within the BES environment and has logical connectivity restricted to only those systems required to perform these activities. Of note is that in the case of VCAs, they must not only be logically isolated from production BES environment network resources, but must also not share any CPU or memory resources with any system within the production BCS environment until the assessment and remediation activities have been completed.

The requirements have been expanded to assure that virtual machines and their associated infrastructure are properly assessed before they are logically connected to a production BCS environment.

Rationale for Requirement R3 Part 3.4

Conforming changes only (see General Considerations for Requirement R3 above).

Former Background Section from Reliability Standard CIP-010-4

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.
Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-010-4

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

---

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

---

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.
With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rationale for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to “model” the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Information Protection

Technical Rationale and Justification for Reliability Standard CIP-011-3

January 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-011-3

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-011-3. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-011-3 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

General Considerations

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-011-3 to align information protection requirements with the virtualization changes.

Requirement R1 and R2

Rationale

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-011-3 for virtualization, the SDT added SCI hosting High or Medium Impact BCS or their associated Electronic Access Control or Monitoring System (EACMS), etc. to each of the Parts in Applicable Systems for Requirement R1 and R2.

Requirement R2 Part 2.1

Requirement R2 Part 2.1 is an objective level requirement focused on protecting BES Cyber System Information (BCSI) rather than 'Cyber Assets' and 'storage media'. This modification creates necessary flexibility, allowing for cryptographic erasure in scenarios where BCSI cannot be mapped to particular disks within virtualized storage, and where BCSI is stored on SCI employing deduplication. This adjustment is also future-looking to better position CIP-011 for the enablement of cloud type scenarios where the disks are owned and/or managed by a third-party as a service to the entity for its BCSI storage, analysis, or use.

Requirement R2 Part 2.2

Additionally, Requirement R2 Part 2.2 is consolidated into Requirement R2 Part 2.1 and the requirement language was modified to an objective level requirement focused on protecting BCSI rather than 'cyber assets' and 'storage media'. This modification allows for cryptographic erasure in scenarios where BCSI cannot be mapped to particular disks in virtualized storage. This approach also sets up Requirement R2 Part 2.2 better for cloud scenarios where the disks are not owned or managed by the responsible entity.

Former Background Section from Reliability Standard CIP-011-2

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.
The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-011-2

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-011-2 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity’s information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity’s BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The SDT’s intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-3

January 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-013-3

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-3. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-013-3 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-013-3 to align supply chain risk management requirements with the virtualization changes.

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-013-3 for virtualization, the SDT added SCI as applicable in Requirement R1. Note that Management Modules of SCI are not added as these are included components that are already covered under of the procurement of the SCI.

Technical Rationale for Reliability Standard CIP-013-2

This section contains a "cut and paste" of the Technical Rationale for CIP-013-2 standard to preserve any historical references.

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

---

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various

---

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

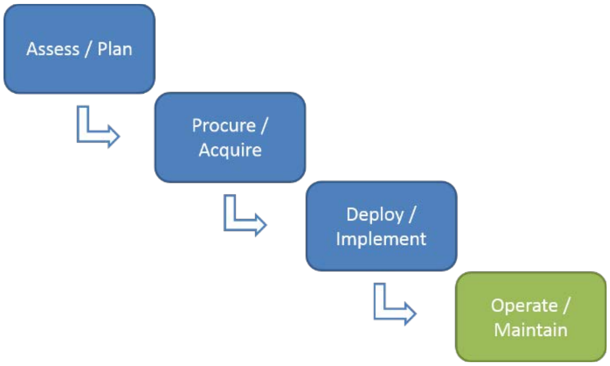
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R3

General Considerations for Requirement R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a “cut and paste” of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

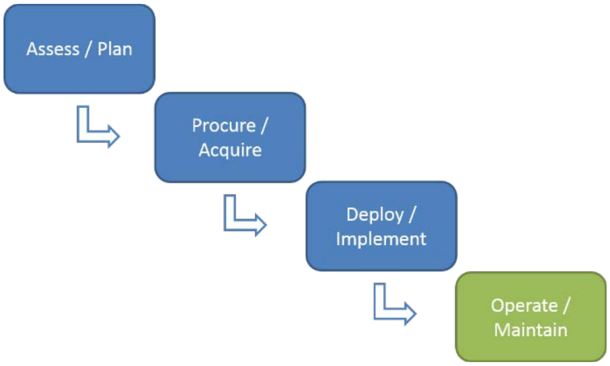
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires

entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.
The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Period Open through March 22, 2021
Ballot Pools Forming through February 19, 2021

Now Available

A 60-day formal comment period for the **CIP Virtualization suite of standards (outlined below)** is open through **8 p.m. Eastern, Monday, March 22, 2021**.

- CIP-002-7 – Cyber Security - BES Cyber System Categorization
- CIP-003-9 – Cyber Security - Security Management Controls
- CIP-004-7 – Cyber Security - Personnel & Training
- CIP-005-8 – Cyber Security - BES Cyber System Logical Isolation
- CIP-006-7 – Cyber Security - Physical Security of BES Cyber Systems
- CIP-007-7 – Cyber Security - Systems Security Management
- CIP-008-7 – Cyber Security - Incident Reporting and Response Planning
- CIP-009-7 – Cyber Security - Recovery Plans for BES Cyber Systems
- CIP-010-5 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-011-3 – Cyber Security - Information Protection
- CIP-013-3 – Cyber Security - Supply Chain Risk Management

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Wendy Muller regarding issues using the SBS**.** An unofficial Word version of the comment form is posted on the project page**.**

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Friday, February 19, 2021.** Registered Ballot Body members can join the ballot pools here. Note that there is a separate ballot and non-binding poll for each of the standards, so it is necessary to join each ballot pool in order to submit votes on all of the standards and their associated Violation Risk Factors and Violation Severity Levels.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Initial ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **March 12-22, 2021**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box. For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name: 2016-02 Modifications to CIP Standards | Virtualization

Comment Period Start Date: 1/22/2021

Comment Period End Date: 3/22/2021

Associated Ballots:
2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 IN 1 ST
2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 IN 1 ST
2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 IN 1 ST
2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 IN 1 ST
2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 IN 1 ST
2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 IN 1 ST
2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 IN 1 ST
2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 IN 1 ST
2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 IN 1 ST
2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 IN 1 ST
2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 IN 1 ST

There were 91 sets of responses, including comments from approximately 210 different people from approximately 133 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT added, revised, and retired several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

2. CIP-005 Requirement R1 part 1.1 was revised to permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

3. The SDT modified CIP-005 Requirement R1 Part R1.2 to establish logical isolation requirements for Management Systems, Management Interfaces, and associated SCI. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

4. The SDT modified CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters. Does the proposed requirement fulfill the directive from FERC Order 791, paragraph 150? Please provide the basis for your response.

5. The SDT modified CIP-005 Requirement R2 to ensure remote access management requirements align with the new and revised virtualization terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

6. The SDT revised CIP-007 Requirement R1 Part 1.1 to shift the security objective from logical network accessible ports to services. The proposed revisions require Responsible Entities to enable only network accessible services that have been determined to be needed by the Responsible Entity. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

7. CIP-010 Requirement R1 currently requires Responsible Entities to develop a baseline configuration, authorize changes to the baseline, and document the changes. The SDT proposes to revise Requirement R1 to remove the reference to baseline configurations. The proposed revisions require the authorization of changes to Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible ports, security patches applied, and SCI configurations. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

8. The SDT modified CIP-010 Requirement R3 Part 3.3 to ensure that vulnerability assessments are performed prior to logically connecting Cyber Assets, VCA, and SCI. The revised requirement allows the use of remediation VLANs to perform active vulnerability assessments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

9. CIP-002-5.1a includes exemption 4.2.3.2, which exempted Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. In the development of conforming changes, the SDT determined that the exemption should be split into two distinct exemptions to adequately cover all cyber systems associated with conforming changes. The SDT

established those conforming changes in proposed Exemptions 4.2.3.2 & 4.2.3.3. Do the changes clearly identify the exempted cyber systems? If not, please provide the basis for your disagreement and an alternate proposal.

10. BCS and SCI are mutually exclusive by definition, however SCI poses a significant reliability risk to the Bulk Electric System. The SDT considered the risks associated with SCI and revised CIP-002 Requirement R1 to include the identification of SCI in Parts 1.3, 1.4, and 1.5. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

11. In the current enforceable standards, there are no requirements that can be used to tie a non-identification of EACMS, PACS, and PCAs to a single requirement. The SDT revised CIP-002 to include the identification of SCI associated with EACMS, PACS, and PCAs to help address this issue within the virtualization scope of the current SAR. The proposed requirement could reduce possible non-compliance to a single issue if a Responsible Entity fails to properly identify SCI associated with EACMS, PACS, or PCAs. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

12. The SDT modified CIP-002 Attachment 1, Criterion 2.1 to align with a previously approved Request for Interpretation (RFI) regarding “shared BES Cyber Systems.” The SDT modified the criterion to reference each discrete shared BCS. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

13. The SDT made conforming changes to CIP-003 and CIP-004. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

14. The SDT modified the Applicable Systems column in CIP-006 to include SCI hosting PACs associated with Medium Impact BCS with ERC or IRA. The SDT made the proposed revisions to clarify the scope of requirements that apply when an entity implements serial IRA. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

15. The SDT made conforming changes to CIP-008 and CIP-009. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

16. The SDT modified CIP-011 Requirement R2 part 2.1, which will allow cryptographic erasure in scenarios where BCSI can’t be mapped to particular disks in virtualized storage. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

17. The SDT performed a review of the CIP Standards and determined that CIP Exceptional Circumstances could be applied to the following additional requirements: CIP-004-7 Requirement R2 Part 2.2, CIP-004-7 Requirement R3 Part 3.5, CIP-006-7 Requirement R1 Part 1.8, CIP-006-7 Requirement R1 Part 1.9, CIP-006-7 Requirement R2, CIP-010-5 Requirement Part 1.2, and CIP-010-5 Requirement R1 Part 1.3. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

18. Implementation Plan: The SDT proposes an Implementation Plan that makes the revised CIP Standards and definitions effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority’s order. However, the implementation plan allows a Responsible Entity to elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. Do you agree with this proposal? If you think an alternate effective date is needed, please provide a detailed explanation of actions and time needed.

19. Please provide any additional comments for the SDT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2016-02 Virtualization	Bobbi Welch	MISO	2	RF
					Ali Miremadi	CAISO	2	WECC
					Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Michael DelViscio	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Portland General Electric Co.	Daniel Mason	6		PGE FCD	Ryan Olson	Portland General Electric Co.	5	WECC
					Nathaniel Clague	Portland General Electric Co.	1	WECC
					Angela Gaines	Portland General Electric Co.	3	WECC

					Daniel Mason	Portland General Electric	6	WECC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					David Hartman	Arizona Electric Power Cooperative	1	WECC
					Jennifer Bray	Arizona Electric Power	1	WECC

						Cooperative, Inc.		
DTE Energy - Detroit Edison Company	Karie Barczak	3		DTE Energy - DTE Electric	Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	4	MRO
					Douglas Webb	Evergy	1,3,5,6	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					Jamie Monette	Allete - Minnesota Power, Inc.	1	MRO
					Jodi Jensen	Western Area Power Administration - Upper Great Plains East (WAPA)	1,6	MRO
					John Chang	Manitoba Hydro	1,3,6	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc.	2	MRO
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO

					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1,3,5	MRO
					Joe DePoorter	Madison Gas and Electric	4	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Duke Energy	Masuncha Bussey	1,3,5,6	FRCC,MRO,RF,SERC,Texas RE	Duke Energy	Laura Lee	Duke Energy	1	SERC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
					Lee Schuster	Duke Energy	3	SERC
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		CHPD	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Ginette Lacasse	Public Utility District No. 1 of Chelan County	1	WECC

					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Sharon Flannery	Eversource Energy	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC

					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Cristhian Godoy	Con Ed - Consolidated	6	NPCC

						Edison Co. of New York		
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable

					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3			Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC

					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The SDT added, revised, and retired several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not generally agree with the proposed modifications. The definitions as currently drafted introduce a complex and difficult matrix of possible “device” identifications that are theoretically mutually exclusive (Cyber Asset, Virtual Cyber Asset, Shared Cyber Infrastructure, Management Modules) and that must then be assigned one or many “roles” (BCA, EACMS, etc.). It may be more straightforward to update the Cyber Asset definition to accommodate multiple technologies including physical or virtual components that comprise the a device (such as hardware, software, and data). The VCA definiation may not be needed if this concept is added to the definition of Cyber Asset. This would avoid introducing another device ‘type’ that is not currently included in applicability statements.

We have concerns that the definition of Management Module may apply to substation devices that have no relationship to virtualiztion. Is the intent to confine use of this term to SCI only? This question may highlight a concern with the approach of defining terms that can only be understood when read in context of the applicability statements.

The proposed definition of Self-Contained Application includes terms such as “isolated” that could be interpreted by regional entities to mean that they would not be allowed network connectivity. Most containers inherently need a network address to perform their purpose. We suggest revising the definition to something like “Packaged software, consisting of binaries that cannot be modified, containing application software, operating system, and all relevant dependencies designed to execute independent of any other software or containers residing on the same infrastructure. SCA may exist on Cyber Assets, VCA, or SCI.”

Duke recommends the SDT add a definition of ‘Logical Isolation’, as that term is central to multiple requirements.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

TVA has concerns with the Share Cyber Infrastructure (SCI) definition: As currently drafted, this term is too vague and could be misinterpreted to extend scope inappropriately.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP would like clarification on the mixed use of CIP and non CIP assets. What components within virtualization becomes an EACMS? Requirements R1 Parts 1.1, 1.2, and 1.3 are a big step from referencing an Electronic Access Point (EAP).

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: The MRO NSRF believes the existing standard requirements could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, reduce the impact to entities' programs, and provide greater clarity to auditors. We recommend reviewing our comments in reply to Question 19 first. This provides an overview basis for our comments in general.

A. SCI - Virtual environments could reside within specified physical security zones thus eliminating the need for a Shared Cyber Infrastructure (SCI) definition. For example, a BCA and PCA supported by the same hardware (server farm, storage system, management system) could be classified as a BCA (high watermarked). Using this logic also eliminates the need to retire the Electronic Security Perimeter (ESP) definition and results in less impact to entities.

B. Logical Isolation - is problematic in that it is undefined. The existing term 'routable protocol' becomes obsolete when 'logical isolation' is used as or in place of an ESP – i.e., to establish an electronic security zone. Logical isolation can expand compliance scope by bringing in non-routable serial connections.

C. VCA - Given no existing specific requirements for a VCA, the SDT could consider modifying the definition of Cyber Asset to include the entire hardware platform hosting the virtual machines. This allows entities to identify and address the appropriate CIP security risks for virtual machines. This also eliminates the need for the term VCA throughout the standards and other definitions, and in entity compliance documentation and processes.

D. Categorization - If an SCI, Management System or Management Module, such as hypervisor host and vCenter, can create, modify, delete or turn off a BCA, it should be identified and categorized in its entirety as a BCA, because it would have an adverse impact on the Bulk Electric System within 15 minutes. Entities whom choose to put many systems in one hardware platform may consider the risks associated with combined systems.

E. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off an EACMS or PACS, it should be identified as EACMS or PACS since it can remove or change the electronic/physical access control functions. This is implied but not clearly stated in the current definition. For clarity, we suggest addressing this gap by modifying the existing definitions of EACMS and PACS.

F. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off a BCA and EACMS, it should be identified as a BCA for the highest-level protection or identified with dual classifications to meet the requirements of both a BCA and EACMS.

Additional Comment: The definition of 'Self-Contained Applications' is problematic in that the current phrase "packaged to execute in an isolated environment" could scope OS installed and managed applications that use a form of virtual isolated containers such as Java Runtime Environment (JRE) that commonly runs an isolated JVM (java virtual machine) that allows local Java code to be compiled into Java Bytecode.

Recommendation: Self-Contained Applications are immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment and **are managed via Management Systems**.

G. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off an EACMS and PACS, the multiple classifications should apply. It should be identified as both an EACMS and PACS and meet requirements of both. The ability for dual classification already exists in the current version. For example, when an EACMS device is located inside an ESP, this device would be also a PCA and should meet the requirements of both EACMS and PCA.

H. Categorization - Where a storage array (raid) is using data and/or information to operate CIP Cyber Assets (rather than solely for backup), the storage array should be identified as a component of the CIP Cyber Asset and meet the same classification as the CIP Cyber Asset. This is a logical conclusion given a CIP Cyber Assets is inoperable without the storage array information and/or data. For mixed trust environments, the high-water marking rule should apply. To keep the storage raid hosting non-CIP data out of CIP scope, non-CIP storage media should be isolated or separated.

RECOMMENDATIONS - Modifications to Existing Definitions (Cyber Asset (CA), EACMS and PACS):

We recommend modifying the definitions of Cyber Asset, EACMS and PACS to eliminate the definitions of SCI, Management System and Management Modules and recommend:

- **Cyber Asset (CA):** Programmable electronic devices, including the hardware, software, and data in those devices. This includes platforms operating virtual machines, which are logical instances of an operating system or firmware hosted on a physical platform.
- **EACMS:** Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems and the Cyber Assets that can create, modify, delete or turn off the above Cyber Assets.
- **PACS:** Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. This includes the Cyber Assets that can create, modify, delete or turn off the above Cyber Assets.

SDT INTENT - Clarity is needed regarding the modifications to definitions of ERC, IRA, IS, PCA, and the retirement of ESP and EAP.

A. If the SDT intended to include non-ESP ERC, modifications to existing ERC definition should include ESP and non-ESP ERC to make it compatible with the existing requirements.

B. If the SDT intended to include non-routable IRA access, a minor modification to the existing IRA can achieve the goal. Actually the current IRA definition has already covered the serially connected devices outside of ESP resulting from (1) the current IRA definition only states the user-initiated access using a routable protocol and doesn't say all communication sessions need to be routable all the way until the end device, and (2) it doesn't say the Cyber Asset that is accessible by a remote client has to be within an ESP. For instance, when a device serially connected to a terminal server and it can be accessible by a remote client, it meets current IRA definition, but current CIP-005-5 R2 doesn't address IRA definition since it only apply to BCS with ERC and missed the serial connected devices.

However, the current CIP-004 R5.1 has implied an IRA definition (for terminations) applies to non-routable EACMS and PACS, where CIP-004 R5.1 requires entities to revoke IRA access to high and medium impact BCS w/ERC and associated EACMS and PACS, it implies EACMS or PACS may have IRA access even though they may not within an ESP- meaning not routable – but you have to revoke the IRA access to them. We suggest changes to IRA to make it clear that the initial access using routable protocol is one of the IRA qualifiers, where the rest of the remote access session can be non-routable.

C. Given the proposed modifications to EACMS listed in this document, the current IS definition could remain unchanged.

D. Definition of ESP and EAP should not be retired since they are still an effective approach for the network perimeter level security controls for physical and virtual machines. Logical isolation is not a defined term is very subjective. If the SDT intended to allow Cyber Asset level security controls, such as using local policies based firewalls, it should be an alternative measure rather than eliminating ESP and EAP approach.

E. If the SDT intended to include non-ESP PCAs, our proposed modifications to PCA can meet SDT's goal.

RECOMMENDATIONS - Modifications to ERC, IRA, and PCA:

- **ERC:** The ability to access a BCS from a Cyber Asset that is outside of the Electronic Security Perimeter in which the BCS resides via a bi-directional routable protocol connection, or the ability to access a BCS that is not within any ESPs from a Cyber Asset through an EACMS controlling communications to and from the BCS via a bi-directional routable protocol connection.
- **IRA:** User-initiated interactive access by a person employing a remote access client or other remote access technology. Remote access originates from a Cyber Asset, using a routable protocol, that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.
- **PCA**: One or more Cyber Assets (1) that are connected to a BCS using a routable within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP; or (2) that are connected to a BCS using a routable protocol where an ESP model is not used and doesn't pass through any EACMS controlling communications to and from the BES Cyber System. The impact rating of Protected Cyber Assets is equal to the BCS it is connected to; (3) that share CPU or memory with a BCA, EACMS or PACS. The impact rating of Protected Cyber Assets is equal to the above highest rated Cyber Asset that shares CPU or memory with the Protected Cyber Assets.

Additional Comment: The proposed definition for IRA does not account for serial connections that have the only user connection point within a PSP and cannot be moved outside of the PSP.

Recommendation: IRA: If the proposed definition for IRA in Question 1 section B of the modifications to definitions of ERC and IRA is not accepted, then there should be an exception included for communications that can only originate within a PSP.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

The proposed definitions are used to significantly expand the number of “Applicable Systems” within the CIP Standards. This leads to a complex applicability section within already complex subject matter. Some of the proposed definitions are mutually exclusive, while multiple proposed terms can apply to a device’s role within the standards. The proposed definitions shift from concepts that are understood by subject matter experts and compliance staff alike, to definitions that are not clear to subject matter experts. The SDT has proposed the retirement of well-known terms such as EAPs and ESPs and added definitions with terminology that includes immutable software binaries, logical instance, and logical isolation. The proposed definitions do not provide industry with a clear understanding of cyber asset applicability. Additionally, the SDT should consider defining logical isolation due to its pervasive use throughout the proposed definitions.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Comments: WAPA believes the existing standard requirements could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, reduce the impact to entities’ programs, and provide greater clarity to auditors. We recommend reviewing our comments in reply to Question 19 first. This provides an overview basis for our comments in general.

1. SCI - Virtual environments could reside within specified physical security zones thus eliminating the need for a Shared Cyber Infrastructure (SCI) definition. For example, a BCA and PCA supported by the same hardware (server farm, storage system, management system) could be classified as a BCA (high watermarked). Using this logic also eliminates the need to retire the Electronic Security Perimeter (ESP) definition and results in less impact to entities.

2. Logical Isolation - is problematic in that it is undefined. The existing term ‘routable protocol’ becomes obsolete when ‘logical isolation’ is used as or in place of an ESP – i.e., to establish an electronic security zone. Logical isolation can expand compliance scope by bringing in non-routable serial connections.

3. The definition of ‘Self-Contained Applications’ is problematic in that the current phrase “packaged to execute in an isolated environment” could scope OS installed and managed applications that use a form of virtual isolated containers such as Java Runtime Environment (JRE) that commonly runs an isolated JVM (java virtual machine) that allows local Java code to be compiled into Java Bytecode.

Self-Contained Apps Recommendation: Self-Contained Applications are immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment and **are managed via Management Systems**.

VCA - Given no existing specific requirements for a VCA, the SDT could consider modifying the definition of Cyber Asset to include the entire hardware platform hosting the virtual machines. This allows entities to identify and address the appropriate CIP security risks for virtual machines. This also eliminates the need for the term VCA throughout the standards and other definitions, and in entity compliance documentation and processes.

1. Categorization - If an SCI, Management System or Management Module, such as hypervisor host and vCenter, can create, modify, delete or turn off a BCA, it should be identified and categorized in its entirety as a BCA, because it would have an adverse impact on the Bulk Electric System within 15 minutes. Entities whom choose to put many systems in one hardware platform may consider the risks associated with combined systems.

2. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off an EACMS or PACS, it should be identified as EACMS or PACS since it can remove or change the electronic/physical access control functions. This is implied but not clearly stated in the current definition. For clarity, we suggest addressing this gap by modifying the existing definitions of EACMS and PACS.

3. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off a BCA and EACMS, it should be identified as a BCA for the highest-level protection or identified with dual classifications to meet the requirements of both a BCA and EACMS.

4. Categorization - If an SCI, Management System or Management Module can create, modify, delete or turn off an EACMS and PACS, the multiple classifications should apply. It should be identified as both an EACMS and PACS and meet requirements of both. The ability for dual classification already exists in the current version. For example, when an EACMS device is located inside an ESP, this device would be also a PCA and should meet the requirements of both EACMS and PCA.

5. Categorization - Where a storage array (raid) is using data and/or information to operate CIP Cyber Assets (rather than solely for backup), the storage array should be identified as a component of the CIP Cyber Asset and meet the same classification as the CIP Cyber Asset. This is a logical conclusion given a CIP Cyber Assets is inoperable without the storage array information and/or data. For mixed trust environments, the high-water marking rule should apply. To keep the storage raid hosting non-CIP data out of CIP scope, non-CIP storage media should be isolated or separated.

RECOMMENDATIONS - Modifications to Existing Definitions (Cyber Asset (CA), EACMS and PACS):

We recommend modifying the definitions of Cyber Asset, EACMS and PACS to eliminate the definitions of SCI, Management System and Management Modules and recommend:

-
    - **Cyber Asset (CA):** Programmable electronic devices, including the hardware, software, and data in those devices. This includes platforms operating virtual machines, which are logical instances of an operating system or firmware hosted on a physical platform.
    - **EACMS:** Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems and the Cyber Assets that can create, modify, delete or turn off the above Cyber Assets.
    - **PACS:** Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. This includes the Cyber Assets that can create, modify, delete or turn off the above Cyber Assets.

SDT INTENT - Clarity is needed regarding the modifications to definitions of ERC, IRA, IS, PCA, and the retirement of ESP and EAP.

-
    i. If the SDT intended to include non-ESP ERC, modifications to existing ERC definition should include ESP and non-ESP ERC to make it compatible with the existing requirements.

    ii. If the SDT intended to include non-routable IRA access, a minor modification to the existing IRA can achieve the goal. Actually the current IRA definition has already covered the serially connected devices outside of ESP resulting from (1) the current IRA definition only states the user-initiated access using a routable protocol and doesn't say all communication sessions need to be routable all the way until the end device, and (2) it doesn't say the Cyber Asset that is accessible by a remote client has to be within an ESP. For instance, when a device serially connected to a terminal server and it can be accessible by a remote client, it meets current IRA definition, but current CIP-005-5 R2 doesn't address IRA definition since it only apply to BCS with ERC and missed the serial connected devices.

However, the current CIP-004 R5.1 has implied an IRA definition (for terminations) applies to non-routable EACMS and PACS, where CIP-004 R5.1 requires entities to revoke IRA access to high and medium impact BCS w/ERC and associated EACMS and PACS, it implies EACMS or PACS may have IRA access even though they may not within an ESP- meaning not routable – but you have to revoke the IRA access to them. We suggest changes to IRA to make it clear that the initial access using routable protocol is one of the IRA qualifiers, where the rest of the remote access session can be non-routable.

iii. Given the proposed modifications to EACMS listed in this document, the current IS definition could remain unchanged.

iv. Definition of ESP and EAP should not be retired since they are still an effective approach for the network perimeter level security controls for physical and virtual machines. Logical isolation is not a defined term is very subjective. If the SDT intended to allow Cyber Asset level security controls, such as using local policies based firewalls, it should be an alternative measure rather than eliminating ESP and EAP approach.

v. If the SDT intended to include non-ESP PCAs, our proposed modifications to PCA can meet SDT's goal.

RECOMMENDATIONS - Modifications to ERC, IRA, and PCA:

- **ERC:** The ability to access a BCS from a Cyber Asset that is outside of the Electronic Security Perimeter in which the BCS resides via a bi-directional routable protocol connection, or the ability to access a BCS that is not within any ESPs from a Cyber Asset through an EACMS controlling communications to and from the BCS via a bi-directional routable protocol connection.
- **IRA:** User-initiated interactive access by a person employing a remote access client or other remote access technology. Remote access originates from a Cyber Asset, using a routable protocol, that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.
- **PCA**: One or more Cyber Assets (1) that are connected to a BCS using a routable within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP; or (2) that are connected to a BCS using a routable protocol where an ESP model is not used and doesn't pass through any EACMS controlling communications to and from the BES Cyber System. The impact rating of Protected Cyber Assets is equal to the BCS it is connected to; (3) that share CPU or memory with a BCA, EACMS or PACS. The impact rating of Protected Cyber Assets is equal to the above highest rated Cyber Asset that shares CPU or memory with the Protected Cyber Assets.

Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
Document Name	
Comment	

Some of the proposed changes are unclear and require clarification to correctly scope requirements. Examples include:

1. ERC – With the new definition the term “external” becomes vague. Since there would be no ESP the entity would have to define “external” to what.

2. IRA - Explanation would be needed to clearly define what a “remote access client” is in a virtual environment.

These are a few of the concerns with the proposed changes which could create a hole in applicability scoping.

Also, the retirement of well-established terms (EAP and ESP) will make entities have to make changes to their CIP program regardless if an entity moves into virtualization or not. Recommend that ESP and EAP definitions be left in the glossary of terms.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

Reclamation recommends the following changes:

- Management Interface should be from within a BES level protected physical location and maintain NERC CIP electronic cyber security controls.
- Include Management Modules within the SCIdefinition..
- Include Management Interface and Modules in BCS definition.

Reclamation also identifies that Self-contained Application is essentially bundled software and may not need to be defined as a new definition within the NERC Glossary of Terms.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	

Comment

EAP and ESP should not be retired terms because they are still acceptable methods for isolating BCS from other assets and will continue to be widely used by entities that do not convert to virtualization or phase it in over time.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

ISO-NE disagrees with the proposed draft definitions. The draft definitions are complex and ambiguous, which could lead to misinterpretations, improper technical implementations and increased risk of non-compliance with the NERC CIP Standards.

ISO-NE believes that the draft definitions introduce a complex and difficult matrix of possible device identifications that are theoretically mutually exclusive (Cyber Asset, Virtual Cyber Asset, Shared Cyber Infrastructure (SCI), Management Modules) and that must then be assigned one or many ‘roles’ (BCA, EACMS, etc.).

ISO-NE recommends that the Standard Drafting Team (SDT) create definitions that are mutually exclusive, do not embed dependencies and references to other definitions for scope, and assign only one role or categorization to a cyber system. It may be more straightforward to update the Cyber Asset definition to accommodate multiple technologies including physical or virtual components that comprise a device (such as hardware, software, and data).

Additionally, ISO-NE disagrees with the retirement of the Electronic Security Perimeters (ESP) and Electronic Access Points (EAP) defined terms. These defined terms are well understood and implemented throughout the industry with known costs and audit expectations. Retiring the ESP and EAP defined terms will require local definition of logical isolation with unknown impacts to programs as well as audit expectations. Maintaining the definitions does not prevent adoption of technology and practice that can enhance security of critical infrastructure. The SDT has publicly commented that the proposed logical isolation requirements allow for backwards compatibility and that an Entity may continue to implement ESPs and EAPs as a form of logical isolation. Therefore, these terms should not be retired and should remain active in the Glossary of Terms Used in NERC Reliability Standards.

The SCI definition seems to address specific scenarios involving storage and/or host virtualization infrastructure, but may be interpreted more broadly to include sets of systems supporting configuration management and monitoring/remediation support systems that may not have been intended for inclusion, e.g. Ansible Tower, Tripwire, and Tenable Security Center. The SDT should consider greater specification of the characteristics of “Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.”

The proposed Self-Contained Application (SCA) definition includes terms such as “isolated,” which could be interpreted by Regional Entities to mean that SCAs would not be allowed network connectivity. Most containers inherently need a network address to perform their purpose.

In addition, the use of “immutable” may be problematic. The definition of Self-Contained Applications containing the term “immutable” does not apply to Containers. A running container can be configured to be ‘mutable’ during the runtime. This may negate containers from the definition. ISO-NE recommends revising the definition to the following suggested language:

“Packaged software, consisting of binaries that cannot be modified, containing application software, operating system, and all relevant dependencies designed to execute independent of any other software or containers residing on the same infrastructure. Self-Contained Applications may exist on Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructures.”

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

We have numerous reasons for voting NO. Several other Entitys' comments show some of our concerns.

After a couple years of Industry and Drafting team laborous discussions and outreach, NERC recent decided to withdrawn CIP-002-6 for FERC's approval and comments. This is a clear sign a Master Plan needs to be created instead of the current numerous different CIP Projects being run with different drafting teams. Too many old and out dated tasks and orders. Soon, and to confuse things more, there will be four CIP drafting teams all changing CIP standards, in most cases the same ones with all different implementation plans. Very confusing, expensive, and administratively budensome for registered entities.

We suggest NERC work with Industry, DOE, and FERC to decide which way to procede with all CIP Standards (develop a Master Plan). Instead of having numerous drafting teams, such as this ones, working on old outdated assignments that will be changed or withrawn in the near future. It seems we are spinning our wheels and getting bogged down in paperwork and cost with no measurable/tangible reliability benefits being realized.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company supports most but not all of the proposed additions, revisions, and retirements of terms. Southern respectfully would like to make the following suggestions for SDT consideration:

1. **Electronic Security Perimeter (ESP)** – Southern requests that the definition of ESP not be retired because the transition (or no transition at all) to virtualization and/or virtualized networks will take considerable amounts of time and effort, and ESPs are still a viable form of logical isolation that can help entities and auditors if it remains active as a defined term. Southern also suggests either referring to ESP’s within a new proposed definition of Logical Isolation, or adding it to the Measures as an example compliance method.

2. **Electronic Access Point (EAP)** – Southern requests that the definition of EAP not be retired because the transition (or no transition at all) to virtualization and/or virtualized networks will take considerable amounts of time and effort, and EAPs are still a viable form of logical isolation that can help entities and auditors if it remains active as a defined term. Southern also suggests either referring to EAP's within a new proposed definition of Logical Isolation, or adding it to the Measures as an example compliance method.

a. Now, taking a step back, Southern request the SDT to also consider:

i. What if the SDT were to retire just the EAP term and then redefine ESP (keep the term) so that it can incorporate a FW on a network edge or a full ZTA "dynamic, encrypted, authenticated, and authorized session" between two objects defined in an access policy without regard to network locations? In other words, static or dynamic "perimeters". Keep the term, just define it at a more objective level than "logical border around a network" and in terms of protecting access to and from a group of applicable assets.

3. **Electronic Access Control and Monitoring System** – Southern requests that the SDT consider that the proposed modifications to the EACMS definition appears to exclude electronic access monitoring by an EACMS of the BES Cyber Systems themselves, but rather that only electronic access monitoring of the logical isolation of those systems is required.

a. *Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of* ***the logical isolation of BES Cyber Systems.*** *This includes Intermediate Systems.*

b. Consider this as an alternative to the EACMS definition: *Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform (1) electronic access control (including Intermediate Systems) or (2) electronic access monitoring of high and medium impact BES Cyber Systems and their associated* ***logical isolation configuration(s)****.*

4. **Logical Isolation** (Undefined Term) – Southern supports the SDT's move toward the use of the term "logical isolation", however, due to its expansive use within CIP definitions and enforceable Reliability Standards, a common understanding and definition of this term is needed to support entity compliance. Southern provides the below suggested language for consideration in this newly defined term:

a. **Logical Isolation:** the implementation of tools, devices, systems, or rules to restrict access and communications to that which is deemed necessary, and deny all other access or communications by default. Examples of Logical Isolation include the implementation of ESPs, EAPs, Zero Trust architectures, affinity rules, etc.

NOTE: *Cyber Security Incident; Electronic Access Control or Monitoring Systems (EACMS); Interactive Remote Access (IRA); Protected Cyber Asset (PCA); Removeable Media; Reportable Cyber Security Incident; Transient Cyber Asset (TCA) are all definitions that require a common understanding of "logical isolation" for it to be correctly implemented.*

5. **Cyber Security Incident** – Southern respectfully requests the SDT consider the following edits to the proposed changes to the CSI definition:

a. A malicious act or suspicious event that:

• For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) a BCS, (2) a Cyber Asset, VCA, or SCI performing logical isolation of a BCS (e.g., EACMS, SCI), or (3) a Physical Security Perimeter; or

• Disrupts or attempts to disrupt the operation of a BES Cyber System

6. **Cyber System** (Undefined Term) – Modifications have been made under the exemptions section in CIP-002-7 which move from a Cyber Asset focus to a "cyber system" focus without a corresponding definition of what that term encompasses. With the difficulty of understanding the scope of this undefined term in virtualized environments, Southern recommends developing a definition for "cyber system", such as:

a. **Cyber System:** one or more Cyber Assets, VCAs, or SCI used to perform or achieve a cyber-based objective by a Responsible Entity or other party.

b. Additionally, Southern requests the SDT to consider that Part 4.2.3.3. should be a sub-set of Part 4.2.3.2. rather than a stand alone item.

7. **Self-Contained Application** - Southern does not support the proposed definition for Self-Contained Application as it is highly technical and ambiguous in nature. Southern requests that the SDT consider the NIST defined term for “Container” below, which we believe is a clearer and more understandable definition for what Self-Contained Application is trying to achieve.

A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container.

Alternatively, consider having no definition for Self-Contained Application and allow CIP-010 R1 to track changes to “application container repositories.” Include in the TR or IG, entities should treat “containers/repositories” like applications and not like Cyber Assets or Virtual Cyber Assets.

8. **Shared Cyber Infrastructure** – Southern does not support the current definition of Shared Cyber Infrastructure for the following reasons:

a. The SCI definition refers to Management Systems used to initialize, deploy, ***OR*** configure, but the definition of Management Systems states that in order to be a Management System it must initialize, deploy ***AND*** configure. The two definitions appear to conflict with each other, and Southern requests that both terms use the ***AND*** conjunction.

b. **Below is a proposed revision:**

i. One or more programmable electronic devices (excluding Management Modules) and their software that share CPU, memory, or storage resources with one or more BES Cyber Systems or their associated EACMS, PACS, or PCA; this includes Management Systems used to initialize, deploy, **and** configure the Shared Cyber Infrastructure.

c. Given the complexity of trying to mix requirements that apply equally to physical Cyber Assets and Cyber Assets hosted on SCI, Southern also requests the SDT consider the possibility of splitting definitions and applicable requirements out further to avoid confusion and still provide forward-looking, objective-based requirements for each scenario. For example – the “V” prefix used below could be a qualifying indicator of “virtual” BCS, EACMS, or PACS.

i. Shared BCS Infrastructure (SBI): For H/M impact V-BCS and associated PCA.

ii. Shared Cyber System Infrastructure (SCI): For V-EACMS, or V-PACS associated with H/M BCS or SBI.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The concept of logical isolation should be defined and added to the glossary of terms. Without defining the concept of logical isolation it will lead to diverse definitions between Entities and Regions.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

During the Feb. 23, 2021 webinar, the SDT pointed out the scope of changes is limited by the SAR (V5 TAG, Order 822). When asked during the webinar, they referenced looking to the Applicable Systems where they tried to keep the proposed changes only to address those items in scope. This can be seen in numerous requirements where Management Modules only "of SCI" have been added when logically the definitions could also apply to Management Modules of any applicable stand-alone system. The SDT explained the definitions are not intended to reach outside of virtualization by bringing in patching or other configuration management systems. This is supported by the rationale presented with the proposed definitions for Management Modules and Management Systems. The proposed definitions for these glossary terms do not align with that limitation.

The Management Modules definition as written clearly includes physical Cyber Assets with out-of-band management ports, which does not align with the SDT intent discussed above.

The Management Systems definition as written would include a Cyber Asset that maintains the integrity of another Cyber Asset, through control of the processes for configuring those assets, which would expand the scope of the definition beyond virtualization.

These inconsistencies between the definitions and intended scope will inevitably cause confusion for industry and auditors. Although the expanded scope of these terms is in the best interest of Cyber Security, the definitions should be revised to match the rationale and only target the intended virtualization scope. The definitions can always be expanded in future Standards Authorization Requests when the scope of change also allows for the SDT to include the applicable stand-alone systems.

Recommendations:

Revise the definitions of Management Modules and Management Systems to limit the scope for purposes of virtualization. Suggested revisions are below.

Management Module - An autonomous subsystem of a [**delete: Cyber Asset or**] Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.

Management Systems - Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of [**delete: Cyber Assets or]** Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.

Revise the definition of Shared Cyber Infrastructure to be consistent with the definition of Management Systems. Suggested revision below.

Shared Cyber Infrastructure (SCI) - One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, **[delete: or**] and configure the Shared Cyber Infrastructure.

We propose to keep the **EAP** and **ESP** as NERC Glossary terms; this will avoid future auditor interpretation issues, allow consistent application of the concepts across industry and preserve backwards compatibility.

We propose the SDT creates a glossary term for “logical isolation” to assist entities and auditors in establishing the scope of this concept as it applies to the CIP Standards.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

The IRA definition shall be review to precise the kind of access that is to be consider IRA. The actual definition doesn’t make a distinction between the engineering access and the access for issuing commands for an operator

Likes 0	

Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question

Likes 0	
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

During the Feb. 23, 2021 webinar, the SDT pointed out the scope of changes is limited by the SAR (V5 TAG, Order 822). When asked during the webinar, they referenced looking to the Applicable Systems where they tried to keep the proposed changes only to address those items in scope. This can be seen in numerous requirements where Management Modules only “of SCI” have been added when logically the definitions could also apply to Management Modules of any applicable stand-alone system. The SDT explained the definitions are not intended to reach outside of virtualization by bringing in patching or other configuration management systems. This is supported by the rationale presented with the proposed definitions for Management Modules and Management Systems. The proposed definitions for these glossary terms do not align with that limitation.

The Management Modules definition as written clearly includes physical Cyber Assets with out-of-band management ports, which does not align with the SDT intent discussed above.

The Management Systems definition as written would include a Cyber Asset that maintains the integrity of another Cyber Asset through control of the processes for configuring those assets, which would expand the scope of the definition beyond virtualization.

These inconsistencies between the definitions and intended scope will inevitably cause confusion for industry and auditors. Although the expanded scope of these terms is in the best interest of Cyber Security, the definitions should be revised to match the rationale and only target the intended virtualization scope. The definitions can always be expanded in future Standards Authorization Requests when the scope of change also allows for the SDT to include the applicable stand-alone systems.

Recommendations:

Revise the definitions of Management Modules and Management Systems to limit the scope for purposes of virtualization. Suggested revisions are below.

Management Module - An autonomous subsystem of a [delete: Cyber Asset or] Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.

Management Systems - Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of [delete: Cyber Assets or] Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.

Revise the definition of Shared Cyber Infrastructure to be consistent with the definition of Management Systems. Suggested revision below.

Shared Cyber Infrastructure (SCI) - One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, [delete: or] and configure the Shared Cyber Infrastructure.

We propose to keep the **EAP** and **ESP** as NERC Glossary terms; this will avoid future auditor interpretation issues, allow consistent application of the concepts across industry and preserves backward compatibility.

We propose the SDT creates a glossary term for “logical isolation” to assist entities and auditors in establishing the scope of this concept as it applies to the CIP Standards.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	No
Document Name	

Comment

CHPD has a concern with the change to the definition of EACMS. The new definition reads, “Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring **of the logical isolation of BES Cyber Systems.** This includes Intermediate Systems.” Previously, the definition stated, “… monitoring **of the Electronic Security Perimeter or BES Cyber Systems**”. The new language excludes devices that perform access control and monitoring of BES Cyber Systems. This will exclude things like AD Controllers, logging servers, etc.

Another concern is the definition of Protected Cyber Asset. CHPD had hoped that the new standards would allow more use of virtualization by clarifying the requirements and making it easier to virtualize a BES Cyber System. Instead, with the phrase “Share CPU or memory with a BES Cyber System; excluding Shared Cyber Infrastructure” in the definition of Protected Cyber Asset it becomes too onerous to even consider virtualizing a BES Cyber System, as simply locating it on the same hardware as a non-BES Cyber System forces all the other VMs to become PCAs. Virtualization of a BES Cyber System was never impossible under the old standards, it was simply the guidance that all VMs would become PCAs that made it untenable, especially for smaller entities who do not have enough BES Cyber Systems to justify separate hardware just for them. It also does not consider network architectures that would mitigate vulnerabilities, such as isolating the virtual cluster from the internet or even the corporate network. The CPU/memory isolation language used in this definition and in other requirements make this draft untenable. Please see question 19 for more on this.

The term “asset” in the definition of IRA is not a defined term and needs to be made clearer. Either “the asset described in CIP-002 Attachment 1” or PSP could be alternatives.

One last concern is the way that scoping has been removed from the definitions. While CHPD could support the removal of scoping from the requirements, it has left the requirement language cumbersome and confusing. Scoping should be kept out of the requirement language and should be limited to the Applicable Systems language, or if that is impossible, left in the definition. For details on this, see comments on CIP-005 R1.2 in question 3.

Likes 0	
Dislikes 0	

Response

Victoria Mordi - Entergy - 3,7,9 - SERC

Answer	No
Document Name	

Comment

In reviewing the redline, there is a reference to “Internet IP” – please clarify

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1

Answer	No
Document Name	

Comment

BC Hydro SME team appreciates the opportunity to review the proposed changes and offers specific comments on the following new terms or modified definitions:

- IRA (Interactive Remote Access): The new definition of IRA no longer limits the applicability to routable protocols only. This may result in some additional communication types to be included in scope like serial over dial-up and potentially could have significant scope impact on BC Hydro's NERC CIP compliance program e.g., this removal of routable only restriction specifically affects Medium Impact BES Cyber BCS with Interactive Remote Access (IRA) and their associated PCA (CIP-005-8 R2.1) and a large number of Medium Impact BES Cyber BCS without External Routable Connectivity assets will come in scope due to this change and expansion in scope to meet the requirement of utilizing an Intermediate System as per the new definition of IRA.

Secondly, we seek clarity on the terms used in the definition of IRA e.g., what is the difference between outside of the asset containing the system being accessed (what is defined as the 'asset') vs. outside of the logical isolation. A typical example is an asset that could be a transmission station or a specific line. If a digital protection relay associated with line has a logical isolation perimeter, would there be concerns with communications from within the station but outside that perimeter, or only with communications from outside of the station completely, as stated in the IRA definition with the specific use of the 'OR' condition.

BC Hydro recommends that the definition of the IRA continues to include the use of the terms related to routing, and suggests that IRA be defined as follows:

"User-initiated access by a person employing a remote access client from outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed, or other remote access technology using a routable protocol."

SCA (Self-Contained Application): We request additional clarification and/or examples on SCA, e.g. examples of immutable software in NERC CIP environment.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Request clarification of Logical Isolation definition. Is the intended definition “The logical border surrounding a VCA associated to a BES Cyber Systems which is connected using a routable protocol”?

Request the review of the EACMS definition or define logical isolation, because the current definition is suggesting that only EACMS are to be used for logical isolation which is not the current case. For example, the usage of an Active Directory could be associated to a BES Cyber System only and not to a logical isolation. Suggest reinstating the “OR”, of the logical isolation Electronic Security Perimeter(s) of BES Cyber Systems or BES Cyber Systems.

Request the review of the Shared Cyber Infrastructure (SCI), the definition seems to define two types of objects; the first object being the server that is sharing the CPU, memory, or storage and the second oject is the console (management system) which is used to initialize, deploy, or configure the Shared Cyber Infrastructure. So in the VMWARE world, the ESX is SCI and the VCenter is a SCI.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved:

Management Module

Management Systems

Self-Contained Application

Shared Cyber Infrastructure

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

Oklahoma Gas and Electric supports the comments provided by EEI.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx

Comment

See attachment for comments.

Likes 0	
Dislikes 0	

Response

Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6

Answer	No
Document Name	

Comment

Basin Electric's concern is that it appears that none of this is applicable to the cloud throughout this project 2016-02 and none of it identifies it as such. This hinders NERC's ability to move forward in the area of cloud based applications. Again - this applies across the board to all questions.

Are they going to keep the concept of EAC and EAMs? Basin would be in support of this depending on how they define and write up EAC and EACMS.

Storage array issue - since storage array wasn't directly impacting assets, this would massively impact Basin Electric - goes against how we have been defining that. PACS on to the storage array - which by these new definitions, the implication would be that we would need separate storage array for assets that are in scope. Inherent separations are there such as encryption, so this would cause quite a bit of additional work here. NERC needs to clearly identify what is contained here.

Section D - logical isolation is not a defined term. We would like to see an actual definition for "logical isolation"

IRA recommendation - would rope in all desktops by definition to Cyber Assets but not BES Cyber Assets. Clarify between BES Cyber Asset - BROS reliability impacts - 15 minute impact; Cyber Asset is all encompassing, programmable electronic devices that include hardware, software.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) suggests that the phrase, “or other remote access technology” does not need to be removed from the Interactive Remote Access definition. The proposed definition for Interactive Remote Access (IRA) seems to dictate a remote access client must be used. Otherwise, entities not using a remote access client would not consider their remote connections to be IRA.

The proposed definition for Intermediate Systems is overly broad and could potentially label other EACMS (such as Cyber Assets controlling two-factor authentication or domain controllers) as Intermediate Systems as these systems aid in restricting IRA. Furthermore, Intermediate Systems do not by themselves restrict IRA. For instance, access control for a Microsoft Windows server acting as a jump host (Intermediate System) is performed by a domain controller.

External Routable Connectivity (ERC) as previously defined using the Electronic Security Perimeter (ESP) implied a degree of separation between a system with ERC and the external world, even though it doesn’t use physical or geographical terms. The new definition removes the words “that is outside of its associated ESP” since ESP is no longer defined. This makes the definition confusing and could possibly be misinterpreted. For example, in a segmented network, each BCS could have ERC to its neighbor in the same rack if traffic is traversing a firewall or router with ACLs defined.

ERC was meant to define access from outside the asset facility, not from the same rack. It is not clear this new definition means what is intended.

CEHE suggests retaining a sense of separation by saying ERC originates from: a) a Cyber Asset not identified in CIP-002; b) an identified Cyber Asset located at another asset; or c) an identified Cyber Asset that is logically separated behind a different EACMS. These criteria may not be airtight, but begin to address this issue, where a BCS could have ERC to its physical neighbor but not to a Control Center that controls it.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

See MEC and BHE comments.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

Southern Indiana Gas & Electric Company d/b/a CenterPoint Energy Indiana South (SIGE) suggests that the phrase, “or other remote access technology” does not need to be removed from the Interactive Remote Access definition. The proposed definition for Interactive Remote Access (IRA) seems to dictate a remote access client must be used. Otherwise, entities not using a remote access client would not consider their remote connections to be IRA.

The proposed definition for Intermediate Systems is overly broad and could potentially label other EACMS (such as Cyber Assets controlling two-factor authentication or domain controllers) as Intermediate Systems as these systems aid in restricting IRA. Furthermore, Intermediate Systems do not by themselves restrict IRA. For instance, access control for a Microsoft Windows server acting as a jump host (Intermediate System) is performed by a domain controller.

External Routable Connectivity (ERC) as previously defined using the Electronic Security Perimeter (ESP) implied a degree of separation between a system with ERC and the external world, even though it doesn’t use physical or geographical terms. The new definition removes the words “that is outside of its associated ESP” since ESP is no longer defined. This makes the definition confusing and could possibly be misinterpreted. For example, in a segmented network, each BCS could have ERC to its neighbor in the same rack if traffic is traversing a firewall or router with ACLs defined.

ERC was meant to define access from outside the asset facility, not from the same rack. It is not clear this new definition means what is intended.

SIGE suggests retaining a sense of separation by saying ERC originates from: a) a Cyber Asset not identified in CIP-002; b) an identified Cyber Asset located at another asset; or c) an identified Cyber Asset that is logically separated behind a different EACMS. These criteria may not be airtight, but begin to address this issue, where a BCS could have ERC to its physical neighbor but not to a Control Center that controls it.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

IRA—The changes to Interactive remote Access (IRA) could use some additional changes. The phrase “outside of the asset containing the system being accessed” seems like it could be removed. Many entities use logical isolation to control access to groups of assets (whether virtual or physical) within the current ESP definition. There shouldn’t be a requirement to control access from each device but simply a requirement to show that there are controls in place to prevent access. This can be done by showing logical or physical isolation, which would include an asset or group of assets. The remaining phrase “from outside of the logical isolation of the system being accessed” appears sufficient to meet this intent.

PCA —The changes to the Protected Cyber Asset (PCA) definition has a phrase that states “that are being actively remediated prior to indroduction to the production environment.” This seems to indicate a compliance activity or compliance requirement and not a compliance definition. It is not clear from this phrase what is being actively remediated. The rationale indicates that it is while the VCA is being prepped from deployment, but there still appears to be a lack of clarity with mixing definitions and activities and this could use some clean up. Additionally, in the previous defintions, PCA was defined as something that was routably connected to a BCS. This newly proposed definition moves to a concept of logically isolated. It is unclear at this time what is expected to logically isolated a devices from a BCS when the devices is serially connected to the BCS. Therefore, it makes it makes it unclear if a device qualifies as a PCA when it is serially connected to a BCS with this proposed definition.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	No
Document Name	

Comment

AZPS agrees with the comments provided by EEI on the proposed additions, revisions, and retirements of terms. A further clarification to the following definitions would be appreciated:

1. Logical Isolation (Undefined Term) – AZPS recommends “logical isolation” be defined. A clear understanding of this term is necessary given that new and revised CIP definitions rely on this term. Additionally, a definition is needed to support compliance.

2. Cyber System (Undefined Term) - AZPS recommends developing a definition for “cyber system”. The exemptions contained within CIP-002-7 have moved from a Cyber Asset focus to one that focuses on the undefined term “cyber system”. The development of a definition for cyber system is needed to provide a common understanding for compliance.

3. Cyber Security Incident; Electronic Access Control or Monitoring Systems (EACMS); Interactive Remote Access (IRA); Protected Cyber Asset (PCA); Removeable Media; Reportable Cyber Security Incident; Transient Cyber Asset (TCA) – AZPS generally supports the revisions of these terms, however, the definitions for these terms rest on a common understanding of “logical isolation”. Logical isolation should be defined prior to implementing these changes.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP agrees with many of the proposed additions, revisions, and retirements of terms. While we support modifications to the CIP Reliability Standards and associated definitions that more clearly accommodate virtualization, it is imperative that legacy solutions remain in the standards for those entities who intend to continue to use those solutions.

AEP generally supports EEI’s suggestions and further suggests that acceptable methods of Logical Isolation including ESP, Zero Trust, etc. should be included in the definition of Logical Isolation and not include these acceptable methods within Measures. These suggestions are listed below.

Electronic Security Perimeter (ESP) – AEP does not support the retirement of this term because some companies may not have immediate plans or ability to move to virtualized networks. While we support changes made to CIP-005, the retirement of the term ESP without some reference to this term within the definition of logical isolation or within the measures within CIP-005 could create confusion. To resolve this concern, AEP requests the term ESP to be referenced within the definition of logical isolation.

Electronic Access Point (EAP) – AEP does not support the retirement of this term because many companies may not have immediate plans or ability to move to virtualized networks. AEP requests similar accommodations as suggested above within our comments regarding ESPs.

Logical Isolation (Undefined Term) – AEP supports the move toward the use of the concept of “logical isolation,” however, due to its expansive use within the Reliability Standards, a definition of this term is needed. In developing a definition, AEP requests that the definition for logical isolation include ESP as an acceptable method of Logical Isolation within a defined term. NOTE: *Cyber Security Incident; Electronic Access Control or Monitoring*

Systems (EACMS); Interactive Remote Access (IRA); Protected Cyber Asset (PCA); Removable Media; Reportable Cyber Security Incident; Transient Cyber Asset (TCA) are all definitions that require a common understanding of "logical isolation" to be fully understood.

Cyber System (Undefined Term) - AEP recommends developing a definition for "cyber system" as a defined term. The Exemptions section contained within all of the proposed CIP Reliability Standards have moved from a Cyber Asset focus to one that focuses on the undefined term "cyber system". The development of a definition for cyber system is needed to provide a common understanding for compliance.

Self-Contained Application - AEP does not support the proposed new definition for Self-Contained Application and questions the need for this term. AEP recommends commonly used and understood IT terms be used. In place of the proposed term, AEP suggests the IT term "Container", which is commonly understood and appears to have the same definition as proposed for "Self-Contained Application".

Shared Cyber Infrastructure (SCI) – AEP does not support the currently proposed definition for Shared Cyber Infrastructure for the following reasons:

- The proposed definition refers to Management Systems used to initialize, deploy, **OR** configure but the definition of Management Systems states that to be a Management System it must initialize, deploy, **AND** configure. These two definitions presently conflict with each other. Before the proposed definition of SCI can be accepted, the identified conflict between this term and its companion term (Management Systems) needs to be harmonized.
- Currently, the scope of SCI is unclear. An explanation of the limiting factors for the scope of SCI regarding their software should be provided, e.g., would the firmware of a server blade be included within the scope of SCI?
- AEP also suggests that the proposed definition would be more easily understood if more language and terms were drawn from current NERC CIP acronyms rather than using their long form names.
- The term SCI may not be clear or fully understood by all entities and we suggest adding examples within the Technical Rationale.

Interactive Remote Access (IRA): While AEP understands the need to streamline the definition of IRA, additional clarification is needed to better describe IRA in the context of virtualization, particularly regarding serial links.

Management Systems: This definition appears to align with the definition of a hypervisor, however, it also includes some language that tries to straddle between both virtualized and non-virtualized environment. This ambiguity may create confusion, and AEP recommends the definition be clarified. It may also be helpful to include some examples of Management Systems within the Technical Rationale.

External Routable Connectivity (ERC): AEP recommends adding "or SCI" at the end of the proposed modification once the definition of SCI is clarified. Current draft reads, "The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset or Virtual Cyber Asset through an Electronic Access Control or Monitoring System controlling communications to and from the BES Cyber System that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection."

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AEPCO is signing on to ACES comments, see below:

ACES feels it's time to address Intermediate Systems (IS) as applicable systems without lumping it in with EACMS. This will allow for more granular controls for IS without having to change other standards and requirements.

On the NERC/SDT webinar, the term "Self-Contained Application" wasn't covered thoroughly. The term is only used in CIP-010, and the definition seems to allude to a software appliance/package such as a virtual firewall, router, etc. Further, if software is running in a truly isolated environment the only security risk would be a physical attack. ACES does not see the need for this Term.

External Routable Connectivity's definition does not read well. Having Cyber Asset or Virtual Cyber Asset in the definition limits scope to those asset classes. The "from" is irrelevant and should be not be limited to any type of device. The definition is founded in communication, not Cyber Assets. Proposed language: The ability to communicate, via a bi-directional routable protocol connection, with a BES Cyber System or Shared Cyber Infrastructure from outside of the BES Cyber System's or Shared Cyber Infrastructure's logical isolation.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

Proposed definitions such as Management Module, Management Systems, Self-Contained Applications, Revised IRA definitions are vague or confusing. Definitions should not rely on rationale documents as a supplement; rather, they should be clear in a standalone format within NERC Glossary of Terms. There appears to be some overlap between the definition of SCI and Management Systems. As the new proposed definitions are used to determine applicability, their clarity is extremely important. We recommend further clarifications be made to these new definitions. As the new/revised definitions are the basis for all the revisions, Hydro One is not able to support the proposed revisions to CIP Standards at this time.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Multiple new terms were added to the standards in this project but not defined within the NERC Glossary of Terms. CIP-005 introduced “controlled communications”, but did not clarify what controlled communications is. Additionally, “System Hardening” was add to CIP-007, but was not defined.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren generally agrees with EEI's comments with some added suggestions. We suggest that logical isolation should be fully defined, and also suggest using the term "logical border" instead of logical isolation. We suggest that assets should be required to have one logical border. In regards to the term Cyber System, Ameren suggests the definition Collection of Cyber Capable Devices. We ask that the SDT not be too prescriptive in their definition, and suggest using the NERC Glossary of terms definition.

We differ with EEI's suggestion for Self-Contained Application because if there's new technology that isn't a container, it could be classified as SCA. Regarding Shared Cyber Infrastructure, Ameren suggests including examples of systems, and we ask that the scope be more defined. Regarding Interactive Remote Access, Ameren believes that the definition provided doesn't make much sense, as current remote workspaces would be considered remote access.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

Definition changes are extremely confusing and do not follow Industry standard terminologies. Many terminologies do not reference BES and hence its extremely confusing.

Furthermore, most new definitions are not required; just BCS definition is sufficient. All other elements must follow, high watermarking and security controls and standards must apply.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Definition changes are not clear and will cause confusion as well as differing interpratations.

Concerns with the definition changes creating a gap in applicable system scope. Proposed defintions appear to create multiple identifiers (SCI, EACMS, Intermediate System, PCA) to the same device.

We suggest keeping the ESP and EAP definitions in the active portion of the glossary.

Does new ERC definition introduce a new Requirement?

Other areas of concern include

- What is the definition of a “remote access client?” 2)
- Need clarification on “outside the asset”.
- Need clarification on the relationship of physical isolation to logical isolation
- Need clarification in regards to Intermediate Systems. The proposed definitions can be interpreted to include firewalls as Intermediate System.
- Need clarification on Management Module and Management Systems
- Need clarification of SCI’s definition. The proposed definition of SCI could include network devices. SCI interpretations say that network services are not SCI.
- Need clarification on Storage. Appears that Storage is a Cyber Asset but not part of a Virtual Cyber Asset. This appears inconsistent.
- Need clarification on Virtual Cyber Asset as a Protected Cyber Asset

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE appreciates the Standard Drafting Team's (SDT's) efforts to establish a framework to specifically address the implementation of virtualized CIP architectures within CIP environments. Nevertheless, Texas RE does not agree that wholesale changes are need to the CIP standards to address virtualization. Instead, Texas RE suggests the SDT consider creating virtualization specific terminology that is applicable to the current overarching CIP framework. Texas RE believes this is best accomplished by (1) amending current CIP definitions to specifically address virtualization concepts; and (2) creating virtualization specific definitions where appropriate. Consistent with this overarching view, Texas RE has the following comments on the proposed definitions:

Electronic Access Control or Monitoring Systems (EACMS)

Texas RE seeks clarification on why the SDT proposed to remove the phrase "or BES Cyber Systems" found in the current approved EACMS definition. Removing this language could inadvertently remove Cyber Assets such as log collectors, SIEMS, and active directories from being identified as EACMS because they do not "*perform electronic access control or electronic access monitoring of the logical isolation of BES Cyber Systems*." Texas RE instead suggests retaining the concept that EACMS include Cyber Assets that perform electronic access monitoring of either logical isolation or BES Cyber Systems to include these devices.

Additionally, Texas RE strongly recommends the proposed EACMS definition retain the five EACMS functions – (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; and (5) alerting – documented in CIP-002-5.1a, recognized by the SDT in the CIP-008-6 project, and documented by FERC addressing enhanced reporting for EACMS performing those five functions. This inclusion will reduce ambiguity by clarifying the functional attributes associated with EACMS.

BES Cyber System Information (BCSI)

The words "ESP names" was removed with no replacement. Texas RE recommends adding the words "Logical Isolation names" to ensure clarity.

Electronic Access Point (EAP)

Texas RE does not agree this term should be retired. Please see the comments regarding CIP-005 in response to the SDT’s Question No. 2.

External Routable Connectivity (ERC)

The current language states “…through an Electronic Access Control or Monitoring System controlling communications...”. If in the scenario, routable protocol is being used but not through an EACMS, then by definition there would be no ERC. Texas RE recommends revising the language to “*The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure that is outside its associated logical isolation via a bi-directional routable protocol connection*.”

Electronic Security Perimeter (ESP)

Texas RE does not agree this term should be retired. Please see the comments regarding CIP-005 in response to SDT Question No. 2. Texas RE recommends defining “logical isolation” for clarity. The undefined term “routable protocol” should be defined to address layer 3 traffic. In part 1.5 further confusion is added by using an uppercase “Internet Protocol (IP)”, which is also not defined. In Texas RE’s experience, these undefined terms have caused interpretation issues in the past. Texas RE therefore recommends limited use of undefined terms in the proposed Standard Requirement revisions.

Interactive Remote Access (IRA)

Removing the words “or other remote access technology”, causes a risk that if a remote access client is not used then it is out of scope for IRA. To address this and ensure a comprehensive IRA definition, Texas RE recommends the proposed IRA definition be revised to read: “User-initiated access by a person employing remote access technology outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed.”

Intermediate Systems

Texas RE recommends the proposed Intermediate Systems definition be adjusted slightly to address the possibility that there could be one or more EACMS used to restrict IRA by adding “(s”) to the EACMS definition. The revised language would read: “*Electronic Access Control or Monitoring System(s) that is used to restrict Interactive Remote Access*.”

Cyber Asset

Texas RE recommends the definition of Cyber Asset be renamed to “Hardware Cyber Asset” to make the distinction with Virtual Cyber Asset.

BES Cyber Asset (BCA)

Consistent with Texas RE’s suggested revisions to the “Cyber Asset” definition to better clarify the distinction between physical and virtual Cyber Assets, Texas RE further recommends that the SDT revise the BCA definition to “A Hardware Cyber Asset or Virtual Machine that” in order to clarify that BCAs include both physical and virtual Cyber Assets.

Virtual Cyber Asset (VCA)

Texas RE recommends aligning the VCA definition set forth in NIST's Computer Security Resource Center glossary as proposed below. The SDT could accomplish this by either addressing the concepts below in the VCA definition itself or creating new definitions.

New term: Virtual Machine.

Definition: A simulated environment created by Virtualization.

New term: Hypervisor.

Definition: The Virtualization component that manages the guest OSs on a Virtualized Host and controls the flow of instructions between the guest OSs and the physical hardware.

New term: Virtualized Host.

Definition: The Hardware Cyber Asset on which the virtualization software such as the Hypervisor is installed. Usually, the Virtualized Host will contain a special hardware platform that assists virtualization - specifically Instruction Set and Memory virtualization. Virtualized Hosts inherit the impact rating and categorization of all hosted Virtual Machines. This phrase would be used instead of Shared Cyber Infrastructure (SCI).

New term: Virtualization.

Definition: The simulation of the software and/or hardware upon which other software runs.

New term: Container

Definition: A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container.

Shared Cyber Infrastructure (SCI)

Texas RE believes that the proposed definition for "Shared Cyber Infrastructure" is too broad in scope. Texas RE reads the current language to include devices normally considered part of the Cyber Asset definition.

Many computer systems are, by design, discrete programmable electronic devices joined together to serve a collective function. This is accomplished by sharing one or more of their CPU, memory, or storage resources with each other. For example, a video card is a programmable electronic device. It shares its CPU and resources with the Cyber Asset it is installed on. As such, it would appear to meet this definition of SCI. Along similar lines, because a data storage virtualization technology (RAID) controllers share their storage resources with the Cyber Assets in which they are installed, such storage technology controllers would also appear to meet this definition. Finally, a computer's motherboard is a programmable electronic device. Its primary function is to facilitate the sharing of CPU, memory, and storage resources between the various discrete devices that have been connected to it. Texas RE respectfully requests the SDT consider these examples in developing an appropriate SCI definition.

Management Modules

Texas RE recommends defining the phrase “autonomous subsystem” as the definition of Management Modules may pull into scope certain devices, depending on how “autonomous subsystem” is defined. For example, some data storage virtualization technology (RAID) controllers provide management and monitoring capability independent of the host system’s CPU, firmware, or operating system. As such, these data storage virtualization technology controllers would appear to meet the definition of Management Module.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

IESO supports TFSIT/NPCC comments.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	No
Document Name	

Comment

The definition of Shared Cyber Infrastructure is open to multiple interpretations as written. The confusion is compounded by the exclusion of Shared Cyber Asset from the definition of Cyber Asset (Cyber Asset itself a problematic definition at times). The intent of the SDT is unclear preventing recommending an alternative proposal.

The definition of Intermediate System is excessively hazy and could be interpreted to mean an authentication system or a Jump host. The intent of the SDT is unclear preventing recommending an alternative proposal.

NERC, including the SDT, needs to be prepared and ensure that adequate CMEP SDT developed guidance is in place to broadly communicate the intent, implementation guidance, and interpretation of the new definitions on passage and prior to NERC Membership and our vendors beginning work to bring systems into compliance. In general terms, WVPA would have preferred that the SDT adopted the terms and directly adapted the definitions used by NIST in their documentation, such as NIST SP 800-125.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

ACES feels it’s time to address Intermediate Systems (IS) as applicable systems without lumping it in with EACMS. This will allow for more granular controls for IS without having to change other standards and requirements.

On the NERC/SDT webinar, the term “Self-Contained Application” wasn’t covered thoroughly. The term is only used in CIP-010, and the definition seems to allude to a software appliance/package such as a virtual firewall, router, etc. Further, if software is running in a truly isolated environment the only security risk would be a physical attack. ACES does not see the need for this Term.

External Routable Connectivity’s definition does not read well. Having Cyber Asset or Virtual Cyber Asset in the definition limits scope to those asset classes. The “from” is irrelevant and should be not be limited to any type of device. The definition is founded in communication, not Cyber Assets. Proposed language: The ability to communicate, via a bi-directional routable protocol connection, with a BES Cyber System or Shared Cyber Infrastructure from outside of the BES Cyber System’s or Shared Cyber Infrastructure’s logical isolation.

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer	No
Document Name	

Comment

FMPA supports the response submitted by TVA.

Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3

Answer	No

Document Name	
Comment	

Portland General Electric Company supports the comments provided by EEI for this survey question.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerns on the definitions may result in a no vote in standards that use those definitions.

Cyber Asset: The current term is “Assets”. The proposed term is “Asset”. The language in the definition is still plural. Solution to make it singular.

Electronic Access Control or Monitoring Systems (EACMS): SDT members have said that VLANS are not allowed because network equipment is not considered SCI since “network services” are not included in what the SCI is sharing. If this is the case, it is difficult to understand why SCI is included in the proposed definition of EACMS.

Need clarification: Is the logical isolation of a Cyber Asset(ie. Windows based firewall) that is part of a system (BCS, Intermediate Systems...) the same as logical isolation of the system? It seems that the Windows based firewall that may be implemented on a Intermediate System or BES Cyber Asset could be considered an EACMS. If this is true then all communication to that Cyber Asset would be ERC.

Electronic Access Point: In order to maintain backward compatibility, this term should not be retired. It has been mentioned that retired terms would be retained in the “Retired Terms” section of the NERC Glossary and therefore not need to be defined by each entity that wishes to use these terms in their compliance documents. It is our view that retired terms and their definitions are no longer recognized by NERC and therefore would have to be redefined by each entity.

Electronic Security Perimeter: This term, or something that captures a boundry between what is protected and what is not protected need to be retained in order to make the “External” in ERC have meaning.

In order to maintain backward compatibility, this term should not be retired In order to maintain backward compatibility, this term should not be retired. It has been mentioned that retired terms would be retained in the “Retired Terms” section of the NERC Glossary and therefore not need to be defined by each entity that wishes to use these terms in their compliance documents. It is our view that retired terms and their definitions are no longer recognized by NERC and therefore would have to be redefined by each entity.

External Routable Connectivity (ERC): The ERC definition used “Electronic Access Control or Monitoring System controlling communications to and from the BES Cyber System”. The Intermediate System definition uses “An Electronic Access Control or Monitoring System that is used to restrict Interactive Remote Access.” It is unclear what the difference is between “controlling” and “restricting”. Solution consistency in language regarding the concept(s).

The proposed definition would make any controlled communication ERC even if that communication is within what would have been the ESP. For examples, an ESP with an internal VLAN would now have ERC for communication between VLANS, communication through a Windows based firewall on a BCA or Intermediate System would be ERC.

Interactive Remote Access (IRA): Does "asset" mean the CIP-002 R1 assets?

Because the network equipment is not clearly excluded from being SCI based on the SCI definition, VLANs could be allowed as logical isolation. Defense in Depth strategies would also create logic isolation within a BCS. Both of these situations could cause IRA to be used for communication performed inside the what was an ESP.

Request clarification on the difference or relationship between physical and logical isolation. The definitions and standards only list logical isolation.

Intermediate Systems: A firewall would implicitly or explicitly restrict Interactive Remote Access that was attempted through it. Therefore, a firewall would be an Intermediate System. This is not consistent with how the term is used in the CIP standards and the security controls that the Intermediate System is intended to provide. Did you intend this definition to be this broad? Example: A router could be Intermediate System based upon the language. Please clarify the intent of this definition.

The term was changed from “System” to “Systems” but the language is still singular.

Management Interface: A Protection System Relay control panel or on/off button may meet this definition. Define monitor. Is a local display, monitoring? Does monitoring require alarms? What do you mean by a physical interface? Why define a term that is only used once in CIP-005-8 R1.2? Suggest that definitions only used in a single requirement should not be defined in the NERC glossary. This would be consistent with the removal of the LERC and LEAP terms.

Is monitoring, as it is used here, consistent with the use in PRC-005?

Management Module: Based on discussions with SDT members, the definition of this term may be based on how it is used in the standards. We believe that all definitions should be clearly written and understood, independent of their use in the standard.

Is it correct that the panel on a Protection System Relay is not a MM because it is not independent of the host systems….?

Does Wake on LAN meet this definition?

Is the Management Module part of the Cyber Asset or is it a separate Cyber Asset? It seems that an autonomous subsystem could be identified as a Cyber Asset.

Please provide some examples of these devices.

Management Systems: Is the use of integrity consistent with its use in CIP-010-5 R1.4? What is the "those assets and systems" referencing at the end? Should it be “Cyber Assets and BCS? Solution “systems” should be removed and “assets” replaced with Cyber Assets and Virtual Cyber Assets.

The Technical Rational restricts this definition to virtual environments but the definition does not include this restriction. It seems that tools such as Ghost, used to image systems, might meet this definition.

Removable Media: What does it mean to be "directly connected .. to .. a network". If thumb drive is connected to a USB port of a PCA but that drive is not shared as a network device, was it connect to the network? What is the difference between "a network not logically isolated from…" and a PCA? Was it the intent of the SDT to remove directly connecting to a PCA?

If I had two BCS each on its own VLAN that all PCA's would be isolated from the other "logical network (VLAN)" and not be Removeable Media if plugged into PCA.

Suggest formatting the proposed Removeable Media definition in the same way that the TCA definition is formatted.

Self-Contained Application: This is only used in CIP-010 R1.1.1 and R1.1.2 for change authorization. Suggest that definitions only used in a single requirement should not be defined in the NERC glossary. This would be consistent with the removal of the LERC and LEAP terms.

Shared Cyber Infrastructure (SCI): In discussions with SDT members, it was stated that VLANs are not allowed because the proposed SCI definition does not include the sharing of “network services”. Some network devices would meet the proposed definition of SCI. The fact that other aspects of these network devices are not listed in the definition does not exclude them from meeting the definition. The proposed definition of SCI must be modified to clearly remove network devices if this is the intent of the SDT.

Transient Cyber Asset (TCA): Not logically isolated would include devices that are physically isolated. Solution clarify the difference between physical and logical isolation.

Need a better understanding of how a VM that spawns for a short period of time is treated. Is the VM image (or whatever it is called) the VCA and not the image or images that are spawned.

The following terms are used but not defined by the SDT.

Logical Isolation: Would like this term defined to include the relationship with physical isolation.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

Southwest Power Pool (SPP) offers the following comments and questions for the SDT consideration of Question 1:

Cyber Asset Definition - The definition of a Cyber Asset is confusing with the exclusion of SCI.

EAP Definition – Consideration that if there is a retirement of EAP, and if we keep with backwards compatibility while using an ESP, we will still need the EAP definition.

ERC Definition - The definition of ERC is confusing because of the introduction of logical isolation. What happens to the IAL network?

IRA Definition - Based on the new definition of IRA, every time you connect to a CIP asset in the same logical isolation area, you are doing ERC. This is not the case in the current version of the standard, and adds a level of confusion.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	
Comment	

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for the definitions. PG&E does have concerns and supports the input provided by EEI.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	
Comment	

During the Feb. 23, 2021 webinar, the SDT pointed out the scope of changes is limited by the SAR (V5 TAG, Order 822). When asked during the webinar, they referenced looking to the Applicable Systems where they tried to keep the proposed changes only to address those items in scope. This can be seen in numerous requirements where Management Modules only “of SCI” have been added when logically the definitions could also apply to Management Modules of any applicable stand-alone system. The SDT explained the definitions are not intended to reach outside of virtualization by bringing in patching or other configuration management systems. This is supported by the rationale presented with the proposed definitions for Management Modules and Management Systems. The proposed definitions for these glossary terms do not align with that limitation.

The Management Modules definition as written clearly includes physical Cyber Assets with out-of-band management ports, which does not align with the SDT intent discussed above.

The Management Systems definition as written would include a Cyber Asset that maintains the integrity of another Cyber Asset through control of the processes for configuring those assets, which would expand the scope of the definition beyond virtualization.

These inconsistencies between the definitions and intended scope will inevitably cause confusion for industry and auditors. Although the expanded scope of these terms is in the best interest of Cyber Security, the definitions should be revised to match the rationale and only target the intended virtualization scope. The definitions can always be expanded in future Standards Authorization Requests when the scope of change also allows for the SDT to include the applicable stand-alone systems.

Recommendations:

Revise the definitions of Management Modules and Management Systems to limit the scope for purposes of virtualization. Suggested revisions are below.

Management Module - An autonomous subsystem of a [delete: Cyber Asset or] Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.

Management Systems - Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of [delete: Cyber Assets or] Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.

Revise the definition of Shared Cyber Infrastructure to be consistent with the definition of Management Systems. Suggested revision below.

Shared Cyber Infrastructure (SCI) - One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, [delete: or] and configure the Shared Cyber Infrastructure.

We propose to keep the **EAP** and **ESP** as NERC Glossary terms; this will avoid future auditor interpretation issues, allow consistent application of the concepts across industry and preserves backward compatibility.

We propose the SDT creates a glossary term for “logical isolation” to assist entities and auditors in establishing the scope of this concept as it applies to the CIP Standards.

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the SRC.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Concerns with definitions could result in NO votes.

Concerns with the definition changes creating a gap in the applicable system scope. The current definitions define scope boundaries (such as ESP, ERC, EAP, IRA) with established demarcations. It is also unclear if multiple identifiers (SCI, EACMS, Intermediate System, PCA) are applied to the same device, causing overlapping scoping requirements (it is unclear of interactions or precedence). The modification or retirement within the proposed definitions causes confusion on the interpretation and application of current and future CIP program-related decisions to remain in compliance.

Request keeping the ESP and EAP definitions in the active portion of the glossary. Having a section for retired terms will not help with compliance. We prefer a clear delineation.

Does the new ERC definition introduce a new Requirement?

ERC comments; 1) request clarification on “external” to what? 2) request clarifications on how VLANs work with ERC 3) request clarification on where the PCAs are 4) Request clarification on physical security, like air gapping, and 5) request that any definition be consistent wherever it is used instead of needing to review the intersection of each definition with each Requirement’s Applicability.

IRA comments; 1) where is the definition of a “remote access client?” 2) request clarification on “outside the asset” – is that referring to CIP-002 R1? 3) request clarification on the relationship of physical isolation to logical isolation.

Request clarification on Intermediate Systems. The proposed definitions can be interpreted to include firewalls as Intermediate System. This would remove the Intermediate Systems requirement as required now and impose additional controls on firewalls that are unnecessary.

Request clarification on Management Module and Management Systems – should the entity internally define “management and monitoring capabilities?” SCI definition use AND while the Management Systems definition uses OR. Request consistency.

Was PCA intentionally removed from the definition of Removable Media?

Request clarification of SCI’s definition. The proposed definition of SCI could include network devices. SCI interpretations say that network services are not SCI.

Request clarification on Storage. Appears that Storage is a Cyber Asset but not part of a Virtual Cyber Asset. This appears inconsistent.

Request clarification on Virtual Cyber Asset as a Protected Cyber Asset.

Request clarification of Logical Isolation definition, is the expected definition be “The logical border surrounding a VCA associated to a BES Cyber Systems which is connected using a routable protocol.

Request the review of the EACMS definition or define logical isolation, because the current definition is suggesting that only EACMS are to be used for logical isolation which no the current case. For example, the usage of an Active Directory could be associated with a BES Cyber System only and not perform logical isolation. Suggest reinstating the “OR”, of the logical isolation Electronic Security Perimeter(s) of BES Cyber Systems or BES Cyber Systems.

Request the review of the Shared Cyber Infrastructure (SCI), the definition seems to define two types of objects; the first object being the server that is sharing is CPU, memory, or storage and the second object is the console (management system) which is used to initialize, deploy, or configure the Shared Cyber Infrastructure. So, in the VMWARE world, the ESX is SCI and the VCenter is an SCI.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 1.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI agrees with many of the proposed additions, revisions, and retirements of terms. While we support modifications to the CIP Reliability Standards and associated definitions that more clearly accommodate virtualization, it is imperative that legacy solutions remain in the standards for those entities who intend to continue to use those solutions. It is from this perspective that EEI offers the following suggestions for consideration.

Electronic Security Perimeter (ESP) – EEI does not support the retirement of this term because some companies may not have immediate plans or ability to move to virtualized networks. While we support changes made to CIP-005, the retirement of the term ESP without some reference to this term within the definition of logical isolation or within the measures within CIP-005 could create confusion. To resolve this concern, EEI recommends the term ESP either be referenced within the definition of logical isolation or a reference to ESPs be included within CIP-005 within Measures.

Electronic Access Point (EAP) – EEI does not support the retirement of this term because many companies may not have immediate plans or ability to move to virtualized networks. EEI recommends similar accommodations as suggested above within our comments regarding ESPs.

Logical Isolation (Undefined Term) – EEI supports the move toward the use of the concept of "logical isolation," however, due to its expansive use within the proposed Reliability Standards a definition of this term is needed. In developing a definition, EEI requests that the definition or measures for logical isolation include ESP as an acceptable method of Logical Isolation. E.g., include in the measures that acceptable methods of Logical Isolation include ESP, Zero Trust, etc. NOTE: *Cyber Security Incident; Electronic Access Control or Monitoring Systems (EACMS); Interactive Remote Access (IRA); Protected Cyber Asset (PCA); Removeable Media; Reportable Cyber Security Incident; Transient Cyber Asset (TCA) are all definitions that require a common understanding of "logical isolation" to be fully understood.*

Cyber System (Undefined Term) - EEI recommends developing a definition for "cyber system". The "Exemptions" section contained within all of the proposed CIP Reliability Standards have moved from a Cyber Asset focus to one that focuses on the undefined term "cyber system". The development of a definition for cyber system is needed to provide a common understanding for compliance. (Questions about the difficulty of defining in virtualized environment.)

Self-Contained Application - EEI does not support the proposed new definition for Self-Contained Application and questions the need for this term. EEI recommends commonly used and understood IT terms be used. In place of the proposed term, EEI suggests the IT term "Container", which is commonly understood and appears to have the same definition as proposed for "Self-Contained Application". NIST defines Container as the following:

A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container.

Shared Cyber Infrastructure – EEI does not support the currently proposed definition for Shared Cyber Infrastructure for the following reasons:

a. The proposed definition refers to Management Systems used to initialize, deploy, **OR** configure but the definition of Management Systems states that, to be a Management System, it must initialize, deploy, AND configure. These two definitions presently conflict with each other. Before the proposed definition of SCI can be accepted, the identified conflict between this term and its companion term (Management Systems) needs to be harmonized.

b. Currently the scope of SCI is unclear. An explanation of the limiting factors for the scope of SCI regarding their software should be provided. e.g., would the firmware of a server blade be included within the scope of SCI?

c. {C}We also suggest that the proposed definition would be more easily understood if language and terms were drawn from current NERC CIP acronyms rather than using their long form names.

d. {C}The term may not be clear or fully understood by all entities and we suggest adding examples within the Technical Rationale.

Interactive Remote Access: While EEI understands the need to streamline the definition of IRA, additional clarification is needed to better describe IRA in the context of virtualization, particularly regarding serial links. While some clarity has been provided within the Technical Rationale regarding serial to IP converter, it is silent on serial links that are used exclusively for polling purposes and have no interactive capability beyond providing requested data.

Management Systems: This definition appears to align with the definition of a hypervisor; however, it also includes some language that tries to straddle between both virtualized and non-virtualized environment. This ambiguity may create confusion, and EEI recommends the definition be clarified. It may also be helpful to include some examples of Management Systems within the Technical Rationale.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - Trevor Tidwell - 1,3

Answer	No
Document Name	

Comment

We have a concern about the definition of SCI. In two places we say "one or more". The problem is what if both statements are answered with one and no more than one. It isn't clear when we say "One programmable electronic device (excluding Management Modules) and its software that share its CPU, memory, or storage resources with one BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets;" What happens when the device itself is a BCS? Is it sharing resources with itself and thus SCI and thus any physical stand alone box is SCI? Consider clarifying that the share is with something besides itself.

The Management Systems definition as written would include a Cyber Asset that maintains the integrity of another Cyber Asset, through control of the processes for configuring those assets, which would expand the scope of the definition beyond virtualization. Please see suggestions from Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 3/19/2021.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	

Comment

Request keeping the ESP and EAP definitions in the active portion of the glossary. Having a section for retired terms will not help with compliance. We prefer a clear delineation.

Request clarification on Management Module and Management Systems – should the entity internally define “management and monitoring capabilities?” SCI definition use AND while the Management Systems definition uses OR. Request consistency.

Request clarification of SCI’s definition. The proposed definition of SCI could include network devices. SCI interpretations say that network services are not SCI.

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1

Answer	No
Document Name	

Comment

Please see JEA coments, an individual response to my comment is not required.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

Intermediate System: N&ST suggests, “An Electronic Access Control or Monitoring System that is used to restrict Interactive Remote Access to only authorized users. The Intermediate System must be located outside the BCS’s logical isolation.”

ERC: N&ST suggests, “The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset or Virtual Cyber Asset that is outside of its associated logical isolation via a bi-directional routable protocol connection.”

Rationale: Clearer and more consistent with the revised definition of IRA.

Management Systems: N&ST suggests, “Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Cyber Assets or Virtual Cyber Assets, through control of one or more of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.”

Rationale: N&ST believes that specifying a system must be capable of managing all three of “initializing, deploying and configuring” in order to qualify as a “Management System” will set the stage for endless arguments about whether a given system does or doesn’t fit the definition. N&ST agrees with the SDT’s opinion that devices used to initialize, deploy, or configure EACMS performing logical isolation should be subject to CIP-005 R1 Part 1.2. However, the proposed definition creates a potential loophole which, we believe, should be eliminated.

Shared Cyber Infrastructure (SCI): N&ST believes the inclusionary language at the end of the proposed definition (“...including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.”) makes the definition confusing and possibly recursive (a Management System used to configure SCI is SCI?). We recommend removing “Management Systems” from the proposed definition. If the SDT believes Management Systems used to configure SCI should be subject to the same set of requirements as SCI, the SDT should consider adding them to the appropriate “Applicability” lists in each Standard.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	

Comment

Please see our answer to #3.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

Cyber Asset should not exclude Shared Cyber Infrastructure. It is just another type of Cyber Asset. Shared Cyber Infrastructure is really a Cyber Asset with a specific purpose.

Cyber Security Incident is written to introduce significant scope creep.

Interactive Remote Access should be reviewed to determine if the language, “User-initiated access by a person employing a remote access client” is still appropriate. There are many implementations that would meet the intent of Interactive Remote Access but may not use a traditional remote access client. If “remote access client” is still necessary, more definition should be provided for the wording.

Intermediate System should retain the wording of access control to restrict Interactive Remote Access to only authorized users. The revision could be unintentionally seen as restricting access from all users. There is no provision in the definition to allow access to anyone.

Virtual Cyber Asset should be clarified to note whether they are required to be on-premises or cloud. If it intended to allow for cloud, it would be beneficial to state that clearly. As written, it could be interpreted that a virtual appliances would be out of scope.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization

Answer	No
Document Name	

Comment

Conceptually, the ISO/RTO Council (IRC) Standards Review Committee (SRC) [1] supports the SDT and its efforts to expeditiously modify the CIP standards to accommodate the use of Virtualization and to more readily be able to adopt other future technological innovations. We believe this will pave the way for increased flexibility, upgradeability and security. In support of the SDT’s efforts, the SRC offers the following comments to assist the SDT in moving forward with this very important initiative.

Recommendation: To ensure entities can continue all or a portion of their existing programs without having to implement virtualization or undertake significant administrative changes, the SRC recommends the terms, Electronic Security Perimeter (ESP) and Electronic Access Point (EAP), be retained as an option for the following reasons:

1) **Ease of backward compatibility**. The concepts of ESP and EAP are well understood and consistently implemented by entities with well-known costs, documentation and audit requirements. Retention of the ESP and EAP concepts will provide a clear path for entities who choose to maintain status quo to remain compliant.

Regardless of whether the terms ESP and EAP are kept, auditors will want/need to know where the logical isolation zone begins and ends.

2) **Continued clarity**. Replacing ESP and EAP with an undefined term, “logical isolation,” will require individual entities to define “logical isolation” with unknown impacts to their existing program and audit requirements. While the IRC SRC sees a benefit to having a more open and flexible definition from the standpoint of being able to more readily adopt new technology and practices that can enhance the security of critical infrastructure, the related cost and compliance risk associated with this change may have the adverse effect of increasing resistance to change in order to avoid audit risk.

The IRC SRC sees a path forward whereby the SDT can introduce the use of the term “logical isolation” in concert with retaining the prior concepts of ESP and EAP by either:

A) Defining the term “logical isolation” to include the terms ESP and EAP as acceptable means of meeting this definition or

B) Reinstating prior language references to ESP and EAP in each applicable requirement and definition in the **Glossary of Terms Used in NERC Reliability Standards** that has been modified to introduce “logical isolation” and offer the prior language as an alternative acceptable means of continuing to comply with the requirement and meet the definition, respectively.

- **Cyber Security Incident** – as noted above, SRC recommends the definition be revised to accommodate prior ESP concepts.
- **External Routable Connectivity (ERC)** – as noted above, SRC recommends the definition be revised to accommodate prior ESP concepts.
- **Interactive Remote Access (IRA)** – as noted above, SRC recommends the definition be revised to accommodate prior ESP concepts.

Clarify the **Management Interface**, **Management Module** and **Management Systems** definitions as they are overly vague.

- **Management Interface** – SRC proposes the SDT narrow this definition to include only those interfaces that can be used to configure Cyber Assets.
- **Management Module** – Describe the type of devices in this category; e.g. out-of-band management devices, I/O devices, etc
- **Management Systems** – per the **Definitions and Exemptions Technical Rationale**, this term is intended to address “the unique risk for virtual environments presented by the management ‘consoles’ for such environments.” It then goes on to say the “intent is to define that capability and then include this within the definition of SCI.”

Recommendation: Clarify where management console servers fall; i.e. under Management Module or Management Systems? Note: the Management Systems definition explicitly excludes Management Modules.

- **Physical Access Control Systems (PACS)** – SRC is concerned that the defintion for PACS could be interpreted to mean that SCI could be solely responsponsible for controlling, alerting or logging access to a Physical Security Perimeter (PSP), even though the word “or” is used to denote that: “Cyber Assets, Virtual Cyber Assets, ***or*** Shared Cyber Infrastructure that control, alert, or log access to the Physical Security Perimeter(s)…”

Recommendation: SRC recommends the following change to the definition to clarify intent:

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that ***collectively*** *control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.”*

- **Reportable Cyber Security Incident** - the “Currently Approved Definition” provided in the CIP Definitions document for Project 2016-02 does *not* match the current definition in the **Glossary of Terms Used in NERC Reliability Standards**; i.e. “*A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity."*

Recommendation: Clarify why it is necessary to change the definition for **Reportable Cyber Security Incident** if the underlying definition for **Cyber Security Incident** is modified. If it is unnecessary, leave the existing definition for **Reportable Cyber Security Incident** as is.

- **Self-Contained Application** – the SRC requests the SDT clarify the nature of “immutable software binaries.” During which stage of the software lifecycle is the software binary expected to be immutable?
- **Shared Cyber Infrastructure** - the definition seems to address specific scenarios involving storage and/or host virtualization infrastructure; however, may be interpreted more broadly to include sets of systems supporting configuration management and monitoring/ remediation support systems. It is not clear whether it was the SDT’s intent to include the latter systems.

Recommendation: Clarify the characteristics of “Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.” Would configuration management systems; e.g. Ansible Tower, Tenable Security Center or Tripwire Enterprise Console be considered Management Systems?

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, PJM and SPP (with the exception of our response to question 5).

Likes 0	

Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC	
Answer	No
Document Name	
Comment	

Capital Power appreciates the opportunity to participate in stakeholder consultation on this project. While Capital Power supports modifications to CIP Reliability Standards and associated definitions that more clearly accommodate virtualization, it is imperative that legacy solutions remain in the standards for those entities who intend to continue to use those solutions.

Shared Cyber Infrastructure (SCI) – Capital Power does not support the currently proposed definition for Shared Cyber Infrastructure for the following reasons:

- The proposed SCI definition refers to Management Systems used to initialize, deploy, **OR** configure but the definition of Management Systems states that to be a Management System it must initialize, deploy, **AND** configure. These two definitions presently conflict with each other. Before the proposed definition of SCI can be accepted, the identified conflict between this term and its companion term (Management Systems) needs to be harmonized.
- Currently, the scope of SCI is unclear. An explanation of the limiting factors for the scope of SCI regarding their software should be provided, e.g., would the firmware of a server blade be included within the scope of SCI?
- The term SCI may not be clear or fully understood by all entities and we suggest adding examples within the Technical Rationale.

Virtual Cyber Asset (VCA) – Capital Power agrees with other stakeholder comments encouraging the integration of the concept of a VCA into a revised definition for Cyber Assets. As there are no additional or specific requirements for a VCA, the integration of this concept into the Cyber Asset definition removes unnecessary complexity.

- Proposed modification to **Cyber Asset (CA):** Programmable electronic devices, including the hardware, software, and data in those devices. This includes platforms operating virtual machines, which are logical instances of an operating system or firmware hosted on a physical platform.

Interactive Remote Access (IRA): The new definition of IRA no longer limits the applicability to routable protocols only. This may result in some additional communication types to be included in scope like serial over dial-up and potentially could have significant scope impact on entities compliance programs. Capital Power recommends that the SDT provide guidance regarding if this was the intent or if the use of the terminology ‘user-initiated’ was intended to point towards routable protocols.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	Yes
Document Name	

Comment

NRG agrees with most of the newly defined and retired terms. However, NRG believes that removing the term, “Electronic Securiry Perimeter” adds a bit of ambiguity and leaves several areas open to interpretation. NRG believes that a new defined term should be added to replace, “Electronic Security Perimeter”. One possible option could be, “Logical Isolation Zone”.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	Yes
Document Name	

Comment

NRG agrees with most of the newly defined and retired terms. However, NRG believes that removing the term, “Electronic Securiry Perimeter” adds a bit of ambiguity and leaves several areas open to interpretation. NRG believes that a new defined term should be added to replace, “Electronic Security Perimeter”. One possible option could be, “Logical Isolation Zone”.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	

Comment

Standards are becoming much more difficult to navigate with this terminology, inclusions and exclusions. The prescriptive nature tends to leave certain high risk Cyber Assets out of scope (vulnerability scanners and Tripwire for example). We do agree that management systems were excluded and that they are high risk, so we support their inclusion.

SMUD was already protecting our SCI without all of this prescriptive language and we do not agree with the 20% of the entities that were polled and said that the standards were holding them back. If this is the direction that the standards are going, we should consider adopting and already developed standard such as PCI rather than reinventing the wheel.

Likes 0	
Dislikes 0	

Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	2016-02_Virtualization_Unofficial_Comment_Form_01222021_gsoc - FINAL DRAFT.docx
Comment	

GSOC provides the following comments regarding the added, revised, and retired defined terms:

1. The definition of BCSI has been revised to include SCI, but not Management Modules or Management Interfaces. It would seem that, at a minimum, information about Management Modules could provide critical information about associated SCI and BCS. GSOC suggests that Management Module should be included in the definition of BCSI. If not, can the SDT provide its explanation for not including Management Module in the definition of BCSI?

2. Relative to Cyber Security Incident and Reportable Cyber Security Incident, both are revised to add the Shared Cyber Infrastructure (SCI), which excludes Management Modules and Management Interfaces, but not Management Systems. Would the attempt to compromise or compromise of an active Management Module in an attempt to access or disrupt the functions of SCI or BCS not merit reporting? This seems like a potential gap where these could be used to compromise related SCI or other cyber assets. GSOC suggests that Management Module should be included. If not, can the SDT provide their explanation or justification?

3. Electronic Access Control or Monitoring Systems should be revised to Electronic Access Control or Monitoring System to comport with its use in its singular form in other defined terms.

4. GSOC provides the following comments on the proposed revision of Interactive Remote Access:

a. The revision of Interactive Remote Access removes the ability to utilize technology other than remote access clients, which seems to militate against the level of flexibility available to facilitate the use of new and advanced technology.

b. The revision of IRA seems to obfuscate whether an “asset” is physical or logical in nature and whether being inside of a trusted network would be considered IRA. Clarification of the SDT’s intent relative to the revision is recommended.

5. The added terms regarding management module, management system, and management interface require some additional clarification to ensure that the distinctions between the new terms are clear and unambiguous. GSOC provides comment relative to the following:

a. Burying management systems in the definition of SCI may create confusion where it is intended to be or should be clearly correlated to other defined terms and requirements. It is recommended that – where such terms are utilized – they should be directly correlated to reduce the potential for confusion.

b. Suggest the following revision to the term “Management Interface” - A physical or logical interface of a Cyber Asset or Shared Cyber Infrastructure with the capability to manage and monitor the hosted Cyber Assets and the Shared Cyber Infrastructure.

c. Suggest the following revision to the term “Management Module” - An autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities of the function and health of the hardware underlying the Cyber Asset or Shared Cyber Infrastructure. This is independent of the host system's CPU, firmware, and operating system and any management or monitoring thereof.

d. Suggest the following revision to the term “Management Systems” - Any combination of Cyber Assets or Virtual Cyber Assets that control the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.

e. Why do Management Modules not require PSP protection?

6. Is the exclusion noted in the definition of a Protected Cyber Asset necessary given that the initial criteria seems to require logical connection and, therefore, would already exclude assets that are not logically connected? Perhaps reformatting of the exclusions would increase clarity. 7. The definition of Self-Contained Application is not easily comprehended or relatable by non-technical personnel. As the reliability standards are intended for use by personnel across the utility industry, including compliance, legal, and other non-technical personnel, revision is recommended to make this defined term more universally understood.	
Likes 2	Oglethorpe Power Corporation, 5, Johnson Donna; Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Maggy Powell - Amazon Web Services - 7

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

2. CIP-005 Requirement R1 part 1.1 was revised to permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO signs on in support of SRC.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization

Answer	No
Document Name	

Comment

Conceptually, the SRC agrees with what the SDT is proposing; however, we don’t think the language is clear enough to implement in practice. Controlled communications are undefined and could require significant effort by entities to interpret and define what is intended and essential to meeting this requirement. What happens if access is over-provisioned because an entity anticipates services are needed and then aren’t used? Due to the vagueness of the language, it seems like this could happen quite readily.

Recommendation: Clarify the definition so there is a level of consistency across the ERO.

In addition, wording such as “e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE)” is difficult to understand.

Recommendation: Replace this language with something in layman’s terms; e.g. “communications for substation automation systems.”

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

Historically CIP-005 has related to the protection of the BCS. This should be the focus going forward. The applicable systems needs to be clarified that it only applies to PACS and EACMS that share infrastructure with something inside the ESP.

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1

Answer	No
Document Name	

Comment

Please see JEA coments, an individual response to my comment is not required.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - Trevor Tidwell - 1,3

Answer	No
Document Name	

Comment

This draft requires PACS and EACMS on SCI to have logical protections, but not for all PACS and EACMS. This allows for human error when applying the standards as people will have to remember which rules apply to which since the rules were not applied in a uniform fashion. Additionally, the elimination of ESP will require extensive modifications to procedure, evidence, RSAWs, etc. Without ESP, how is the logical electronic security perimeter expressed?

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

NERC glossary term needed. The term 'logical isolation' is used in a range of different contexts across many industries. Is it similar to 'deny by default'? Is an ESP a subset of 'logical isolation'?

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Conceptually, the proposed change to only permit needed and controlled communications to and from applicable systems either individually or as a group is clear, however, it is unclear what it means to logically isolate all other communications. A clear understanding of the term logical isolation is needed to address this concern.

Additionally, EEI asks for clarification for the following:

- EEI asks for clarifications of the term “group” as used in Requirement R1, part 1.1. Currently, the Requirements of CIP-005-6 allow multiple BES Cyber Systems to exist within the same Electronic Security Perimeter. However, our understanding of proposed CIP-005-8 is that, when two or more BES Cyber Systems are 1) located within a Control Center; 2) utilizing a shared ESP; and 3) compliant under the current version of CIP-005, they may not be compliant under the proposed Requirements of CIP-005-8. This understanding is based on the potential inability to demonstrate control of communication between the two BES Cyber Systems. While we recognize that the intent may have been for those systems to be considered as part of a group, this is not clearly defined or explained. Without such clarification, entities may find it difficult to continue to use legacy systems under the proposed new Requirements.

- Applicability: PACS and EACMS are included when “hosted on SCI”. It is unclear whether PACS or EACMS hosted on standalone hardware would also meet this requirement. We recommend the language be clarified in proposed CIP-005 Requirement R1 part 1.1. (EEI also recommends evaluation of this issue with respect to R1.3, R1.4 and R1.5)
- Measures: EEI understands that if a VLAN is an acceptable logical isolation technique, then the device enforcing the VLAN would also need to be addressed. EEI requests clarification where these devices are within the proposed standard. (E.g., a switch with a VLAN that has a BCS connected to it. Would that switch be a high impact BCS? Or possibly SCI?) Please clarify how this concern has been addressed within the propose language of R1.1.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 2.

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the SRC.

In addition, PJM requests additional clarification on the “time-sensitivity” aspect of R1.1. This clarification may help entities determine any applicable exceptions.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed such that the entity first identifies needed communications, thenapplies control of the permitted communications.

Suggested language for R1.1 -

Identify needed communications and control permitted communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Likes 0

Dislikes 0

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-005, R1, Part 1.1. PG&E does have concerns and supports the input provided by EEI.

Likes 0

Dislikes 0

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

SPP offers the following comments and questions for the SDT consideration for Question 2:

How would an entity logically isolate from its systems if the term ESP is removed? Recommend SDT consideration that there is no difference, but would require additional documentation and explanation on how network isolation is done, unless we define the two IP addresses as the isolation.

Recommend the SDT consider a definition of what Logical Isolation is, or offer clearly communicated examples.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerns on the definitions caused this no vote for this standard.

Would like clarification on if physical isolation is considered a type of logical isolation and if not, if it should be added as an applicable security control.

Would like clarification why the SDT choose to use “needed”, instead of “necessary” as used in CIP-003 R2 Attachment 1,Section 3.

There has been considerable push by some regions to have phone systems identified as BES Cyber Sytems. In their push, they want the possible threat of someone using calling in and pretending to have the authority to issues operational directives, to be considered in the BCS determination process. While we do not agree with this position, boic communication would be applicable for the R1.1 controls. Suggest including language that clearly exempts voice communication.

Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question.

Likes 0	

Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	
FMPA supports the response submitted by TVA.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
There is a lack of clarity around the expectation related to use of the term needed. If the intent of the SDT is to continue requiring documentation of “needed” communications, this should be converted to an explicit requirement stating the expected documentation rather than an implied requirement. If the intent is to continue the V5 expectations, document the communications services that are permitted (e.g. TCP ports, UDP ports, IP proctocols) with reason access is needed. If the intent is broader to address items such as services in a hypervisor, VLANs, VXLANs, it is not clear what is expected and appropriate language should be developed by the SDT. Further, when considering logically isolated networks that span multiple PSPs connected via a telecommuncations company, configuration is often not in the control of the entity.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI	

Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
The term controlled communications is not defined and open to interpretation. Is a router capable of performing controlled communications? Auditors may have differing opinions.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
There is no need to change a pre-established definition such as ESP. New application creates extreme confusion for application of security for cyber assets. Compartmentalization should be based on security enclaving but high watermarking. A VLAN should be highwater marked to Cyber Asset level as BES function will be impacted if it is compromised. **It seems SDT has compartmentalized assets in order to limit compliance application. Selective application of controls will result in significant security risks.**	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	

Ameren agrees with and supports EEI's comments.

Likes 0

Dislikes 0

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

The Applicability in CIP-005 R1 Part 1.1 may contain a hall of mirrors for EACMS requiring an EACMS with the inclusion of “3. EACMS hosted on SCI” under the High and Medium Applicable Systems entries. One possible solution is to modify the inclusion to be something like:

“3. EACMS, not performing logical isolation, hosted on SCI.”

This would then become the corollary to the R1 Part 1.2 “EACMS performing logical isolation” inclusion. This change could solve the hall of mirrors and serve the security objective of requiring logical isolation of EACMS like Active Directory, where you can without requiring an EACMS for an EACMS that provides logical isolation.

Likes 0

Dislikes 0

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

The term “controlled communications” is new and is not defined. This term could be interperted in many different ways and does not have an industry accepted usage..

Likes 0

Dislikes 0

Response

Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	

AEP is concerned that the proposed change in CIP-005 Requirement R1 Part 1.1 is not clear without a clear understanding of the term logical isolation.

AEP supports EEI's comments and asks clarification on the Applicability where PACS and EACMS are included when "hosted on SCI". It is unclear whether PACS or EACMS hosted on standalone hardware would also meet this requirement. Would this only be applicable if the SCI is hosting BCS or PCA that are mixed with PACS and EACMS on the same hardware? AEP recommends the language be clarified in proposed CIP-005 Requirement R1 part 1.1. AEP also recommends addressing this issue in R1.3, R1.4 and R1.5.

Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	

AZPS agrees with the proposed change to only permit needed and controlled communication to and from appliable system wither individually or as a group is clear. We would like a clearer definition and understanding of what the term "logical isolation" means.

Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

The wording of the requirement is not clear. It states that entities are to permit only the needed and controlled communications but then goes on to state “logically isolate all other communications”. If only the needed communicates are allowed, what communications are being isolated? Other communications to non-CIP devices or systems? And why would this statement be needed? This would still be captured within the phrase of permit only the needed and controlled communications. Is the intent to prevent all other communications other than what is needed or to create a VPN or to encrypt the communication path? Additionally, the applicable systems column is not clear. Does the addition of routable protocols to the High Impact systems mean that if a High Impact system only has serial protocols (while unlikely) this requirement would not apply? This also creates another tier of systems: High with routable, High without routable, Medium with routable, Medium without routable, low, etc. Continuing to create tiers within the requirements complicates the requirements from an administrative standpoint without major security gains. Also, does the phrasing “hosted on SCI” for both PACS and EACMS mean that if a PACS or EACMS is not hosted on SCI that this requirement does not apply? Is this requirement only intended to apply to

virtualized environments? The technical rational speaks heavily to logical isolation, but the requirement language and the language used in the applicable system column don’t seem to completely line up.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not agree with the proposed changes of adding virtual PACS and EACMS to the applicable systems since it expands the scope of the requirement. There is no documented reason for the scope increase. SIGE assumes that this change may be due to the possibility that BCS, PACS, and EACMS may use the same SCI. If that is correct, then SIGE proposes more specific language such as “PACS hosted on SCI that also hosts BCS; and EACMS hosted on SCI that also hosts BCS”.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	

CEHE does not agree with the proposed changes of adding virtual PACS and EACMS to the applicable systems since it expands the scope of the requirement. There is no documented reason for the scope increase. CEHE assumes that this change may be due to the possibility that BCS, PACS, and EACMS may use the same SCI. If that is correct, then CEHE proposes more specific language such as “PACS hosted on SCI that also hosts BCS; and EACMS hosted on SCI that also hosts BCS”.

Likes 0	
Dislikes 0	

Response

Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6

Answer	No
Document Name	

Comment

Proposed changes to R1 Part 1.1 are not required because the ESP concept can still be used with virtualization as one of the options.

Does a zero trust model make it difficult to do virtualization in other ways?

Would segmentation technology count as the control or as the firewall?

An ESP for each microsegmentation would be daunting to any entity.

Logical isolation is not a defined term. We would like to see an actual definition for "logical isolation"

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx

Comment

See attachment for comments.

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
The prior definition defined traffic as ERC, then had a requirement to pass that through an EACMS. The new definition adds ‘through an EACMS’ as a qualifier of the traffic, but falls short of requiring the traffic to pass through an EACMS. (Traffic not going through an EACMS would then not meet the definition of ERC, so the applicable requirements would then not apply.) Consider replacing ‘through an EACMS’ with ‘across logical network isolation’.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The appears to be some ambiguity of the additional compliance requirements which are correlate to the new terms which need to be more defined.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

What are intelligent electronic devices ? Please use define terms.

The requirement doesn't clearly state the creation (establish) of the logical isolation. The requirement should estasblish the logical isolation. In this context logical isolation is not define nor specified.

Suggest removing any reference to "communications using protocol IEC TR-61850-90-5 R-GOOSE" and simply state " excluding time-sensitive protection or control functions".

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	No
Document Name	

Comment

CHPD approves of the direction of performing logical isolation at either the individual or group level instead of requiring an ESP.

However, including PACS and EACMS hosted on SCI in the Applicable Systems creates differing requirements for virtualized PACS and EACMS and physical devices. It is also not backwards compatible with entities who have already virtualized PACS or EACMS and are compliant today but would not be under the draft requirements. Given that the SDT acknowledged during its recent webinar that the only reason it has not extended this requirement to all EACMS and PACS is that it would be outside the SAR, it is clear that this is not a virtualization-based change and is outside the SAR. Additionally, it creates an issue where the device performing the logical isolation of the EACMS or PACS is not a CIP device, and is not required to comply with the CIP standards, creating a hall of mirrors situation, such as a virtual firewall providing logical isolation for a domain controller (but not for any BCS).

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed such that the entity first identifies needed communications, thenapplies control of the permitted communications.

Suggested language for R1.1 -

Identify needed communications and control permitted communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture. I have a request for additional information from the Standards Drafting Team to get clarity.

Likes 0

Dislikes 0

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question

Likes 0

Dislikes 0

Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
The relationship between logical isolation versus the physical security perimeter or its extension through secure conduits is unclear. The notion of zone isolation and conduits (IEC62443) is absent or too abstract. Conduits or secure tunnels between two endpoints (which are secured by a physical perimeter) is not clear.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed such that the entity first identifies needed communications, then applies control of the permitted communications.

Suggested language for R1.1 -

Identify needed communications and control permitted communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

RF does not agree with the proposed changes for the following reasons:

a. With each system becoming its own ESP (zero trust) – mixing of CIP and non-CIP network traffic on local network segments is permitted.

b. Logical isolation is not defined, leading to diverse definitions between entities and regions, therefore, a definition of logical isolation is required. In addition, a significant concern is that an entity could implement logical isolation using only a host-based firewall and essential systems could be directly connected to the internet – a side effect breaking the definition of External Routable Connectivity and enabling entities to bypass many now-required protections.

c. The use and definition of “controlled communications” within P1.1 is not defined. The SDT inferred access control, however, this should be explicitly stated in the Requirement.

d. Remediation VLANs are not defined and may introduce situations where an entity could inadvertently place production Cyber Assets in this VLAN.

e. Dormant VMs that could be either explicitly or inadvertently activated could lead to noncompliance if they are not properly identified.

f. Parent Images and Parent/Child Images are not defined terms and could lead to compliance issues regarding network access and/or identification of Cyber Systems.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern agrees with the concept of only permitting, either individually or as a group, needed and controlled communications to and from Applicable Systems. However, the full intent and scope of “logically isolate all other communications” is unclear absent a defined term for “Logical Isolation”. This issue may be resolved by defining Logical Isolation and providing a clearer understanding of what is required here.

Additionally, Southern requests clarification for the following:

1. Applicability: PACS and EACMS are included when “hosted on SCI”. However, those devices are also included in the definition of SCI; thefore, the requirement language equates to the following applicability:

a. This requirement applies to PACS and EACMS hosted on programmable electronic devices that share their software, CPU, storage, or memory resources between those hosted PACS or EACMS *AND* one or more (1) H/M BCS ***OR*** their associated (2) EACMS, (3) PACS, or (4) PCA.

b. Southern requests the SDT consider the concepts outlined in the following clarifying changes to the Applicable Systems column, which helps clarify the vastly broadening scope of these requirements to EACMS and PACS assets not previously required. This is potentially a major change, but is supported by our other comments in this posting addressing the lower risk profile posed by PACS assets and EACMS assets that only perform a monitoring function. The intent here is to more properly scope risk where stand-alone virtual PACS and EACMS on SCI are of a significantly lower risk than SCI hosting BCS (and virtual PACS on the same SCI). From a risk-based perspective, please consider these associations for Applicable Systems:

i. High and medium impact BCS connected to a network via a routable protocol and their associated:

1. PCA;

2. PACS hosted on the same SCI as the BCS; and

3. EACMS hosted on the same SCI as the BCS.

c. Southern requests the SDT consider the potential “Hall of Mirrors” that is achieved when the object of the requirement (an EACMS) that is used to “permit” and “logically isolate” communications is also subject to having the requirement enforced on itself as an Applicable System. For example – with an EACMS being the object of the requirement, how then does an entity also concurrently use a Cyber Asset(s) (i.e., a 2nd EACMS) to “permit” and “logically isolate” communications to the 1st EACMS?

i. This is exponentially more complicated in a virtualized environment and could force entities, who would not be able to achieve the requirement, to forgo the benefits of virtualization as this would result in endless amounts of dedicated virtual clusters on dedicated hardware for each Applicable System type.

Likes 0

Dislikes 0

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0

Dislikes 0

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

ISO-NE generally agrees with the proposed changes. The logical isolation requirements provide flexibility and a pathway to adopt technology and practices that can enhance security of critical infrastructure. However, ISO-NE recommends several changes to improve comprehension, readability, and compliance with the requirements.

The SDT should define the term “controlled communications” for a consistent interpretation across the industry and Electric Reliability Organization (ERO). Undefined terms create varying definitions and interpretations that can lead to disputes and disagreements between a Registered Entity and the Regional Entities that represent the ERO.

ISO-NE also recommends removal or replacement of the word “ensure” as this language and expectation is inconsistent with all other requirements.

Likes 0

Dislikes 0

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	
Comment	
The phrase "Logically isolate all other communications" should be further explained or clarified. As written, this could lead to incorrect assumptions or interpretations. Logical isolation should be defined as well.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends a change control board process that any new communication to and from applicable BCS needs approval by a responsible individual (not the CIP Senior Manager) to ensure a proper change control process has been applied to key equipment that allows remote access from outside the BCS controlled perimeter or zero-trust model.	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
Document Name	
Comment	
In theory the concept is good, however, more clarification on the relationship between logical isolated zones and physical isolated zones will be required.	
Likes 0	
Dislikes 0	

Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

Comments: The proposed changes to R1 part 1.1 are not required because the existing ESP language and concepts can still be used with virtualization.

1. The language "Permit only needed and controlled communications to and from applicable systems" is problematic because it exceeds what the SAR requires. This language is more based in security defense in depth (multi-layered security controls) but for CIP, routable protocol traffic control between CIP Cyber Assets within the ESP is not required.
2. If the SDT intended to allow a non-ESP model (e.g., zero trust model) for controlling routable protocol electronic communications ingress or egress a BCS, adding EACMS as an alternative option for CIP-005-6 R1.1 could resolve this issue. For instance, in the VMware zero trust model, VMware NSX using a transparent in-kernel stateful firewall to block traffic between VMs, the NSX platform could be identified as an EACMS resulting from our proposed EACMS revisions.

The rationale for discussing logical isolation is as follows:

- The logical isolation is not a defined term and very subjective and can be interpreted differently;
- For routable connectivity, ESP and EAP as one of the options still would apply to a VCA and can be used seamlessly based on existing language and concepts. The term logical isolation is not needed
- For the non-routable connectivity, the objective of the SAR was to address IRA related serial connection issues, which can be resolved by our proposed IRA revision (See our comment for QUESTION 1). Except for IRA related non-routable connectivity, the logical isolation between CIP Cyber Assets using layer 1 and layer 2 connectivity is not required by the SAR.

RECOMMENDATION: We suggest keeping the applicable systems and making the following change to the CIP-005-6 R1 part 1.1

- All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP, or
- All applicable Cyber Assets connected to a network via a routable protocol shall through an EACMS that denies all communications to and from other Cyber Assets by default if ESP model is not used.

Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	

Comment	
The proposed revision to CIP-005 R1.1 is clear with the exception of "controlled communications." If an entity permits needed communications via an ACL, does that mean it is controlled? The requirement text starts with "Permit only needed…" which appears to make "controlled" unnecessary. Additionally, logical isolation is not defined and is subject to interpretation.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

Comments: The proposed changes to R1 part 1.1 are not required because the existing ESP language and concepts can still be used with virtualization.

A. The language "Permit only needed and controlled communications to and from applicable systems" is problematic because it exceeds what the SAR requires. This language is more based in security defense in depth (multi-layered security controls) but for CIP, routable protocol traffic control between CIP Cyber Assets within the ESP is not required.

B. If the SDT intended to allow a non-ESP model (e.g., zero trust model) for controlling routable protocol electronic communications ingress or egress a BCS, adding EACMS as an alternative option for CIP-005-6 R1.1 could resolve this issue. For instance, in the VMware zero trust model, VMware NSX using a transparent in-kernel stateful firewall to block traffic between VMs, the NSX platform could be identified as an EACMS resulting from our proposed EACMS revisions.

The rationale for discussing logical isolation is as follows:

- The logical isolation is not a defined term and very subjective and can be interpreted differently;
- For routable connectivity, ESP and EAP as one of the options still would apply to a VCA and can be used seamlessly based on existing language and concepts. The term logical isolation is not needed
- For the non-routable connectivity, the objective of the SAR was to address IRA related serial connection issues, which can be resolved by our proposed IRA revision (See our comment for QUESTION 1). Except for IRA related non-routable connectivity, the logical isolation between CIP Cyber Assets using layer 1 and layer 2 connectivity is not required by the SAR.

RECOMMENDATION: We suggest keeping the applicable systems and making the following change to the CIP-005-6 R1 part 1.1

- All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP, or
- All applicable Cyber Assets connected to a network via a routable protocol shall through an EACMS that denies all communications to and from other Cyber Assets by default if ESP model is not used.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP has a concern as the requirement is written for Vitural environment, and we do not see in the requirement where it written for the backward compatibility and no reference to the current standard.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Consider alternative wording to clarify the treatment of time-sensitive protections and control functions: *Permit communications that are needed to and from applicable systems either individually or as a group and isolate them from other communication channels. Exclude devices that communicate using control functions (power system automation) or time-sensitive network (TSN) protections (e.g, IEC 61850, GOOSE, SV, PTP)*

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy does not generally agree with the proposed modifications. The verbiage within this requirement appears to be too vague for consistent implementation. The Requirements must be made clear that current ESP models are compliant. Duke Energy suggests including examples in the Measures column that are consistent with current ESP definitions to reinforce that current approaches remain valid.

The proposed language leaves possibility for auditors to disagree with entity application of controls and enforce controlled communications within existing "groups" defined by current ESP boundaries. Duke Energy suggests clarifying as follows "Identify and document logical isolation for applicable systems individually or in groups, and only permit needed and controlled communications across the identified isolation, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE)."

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	Yes
Document Name	

Comment

What are intelligent electronic devices? Please use define terms.

The requirement doesn't clearly state the creation (establish) of the logical isolation. The requirement should establish logical isolation. In this context, logical isolation is not defined nor specified.

Suggest removing any reference to "communications using protocol IEC TR-61850-90-5 R-GOOSE" and simply stay to excluding time-sensitive protection or control functions.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	Yes
Document Name	

Comment

AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
LCRA is concerned with the conecept of backwards compatibility and Regional Entities interpretation of what acceptable evidence is.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC provides the following comments regarding CIP-005, requirement R1: 1. In the proposed revisions for CIP-005, for applicable systems, it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., “…hosting [] impact BCS and the BCS’s associated …..” or “….hosting [] impact BCS and the SCI’s associated…..” 2. Revise requirement R1.1. for clarity as follows: Permit only controlled communications that are [necessary/needed] to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE is concerned with removing the terms Electronic Access Point (EAP) and Electronic Security Perimeter (ESP) from the NERC Glossary of Terms without adequately addressing those concepts in the proposed “logical isolation” definition. The EAP and ESP concepts are known throughout industry and have been further clarified through repeated compliance engagements. As noted in its response to SDT Question No. 1 above, Texas RE believes that registered entities can implement virtualized environments within the existing EAP and EACMS framework today. The SDT is proposing to remove these terms and replace it with the term “logical isolation,” which does not have a proposed definition. Texas RE recommends the SDT define the term “logical isolation.” In doing so, Texas RE further suggests the SDT clarify that the EAP and ESP concepts apply as part of the overarching “logical isolation” concept. Finally, Texas RE recommends retaining the measure language, which states: “*a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP*.”	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	

Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

3. The SDT modified CIP-005 Requirement R1 Part R1.2 to establish logical isolation requirements for Management Systems, Management Interfaces, and associated SCI. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Consider revising Parts 1.2.1 and 1.2.2 to clarify controls for "Management Systems" and "Management Interfaces." The proposed language in Part 1.2.2 could be inappropriately interpreted to imply the management plane must have its own hypervisor.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The inclusion of virtualization concepts with newly defined Applicable Systems makes the requirements harder to understand and identify what is truly applicable. SRP doesn’t like how all the standards increased in size due to these additions. SRP prefers to implement a way to account for virtualization without sweeping changes – similar to Low Impact. The attention given to virtualization feels over weighted compared to non-virtualized systems. This increases the burden on entities without virtualization to comb through the standards to find what is applicable.

The requirement is written for Vitural environment, and SRP doesn’t see in the requirement where it written for the backward compatibility and no reference to the current standard.

SRP would like clarification on how the applicable systems, in particular EACMS, are expanded because of the SCI term.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: We believe there are more efficient methods to meet the SAR. Refer to the comments in QUESTION 1 regarding existing definitions.

The term “Management Interface” already exists in the inherent properties of a Cyber Asset in the manner in which a Cyber Asset connects to the network – i.e., copper, fiber, wireless, etc.… If the intent was to address access to a Cyber Asset, the existing language covers these controls in electronic access – ports and services and authentication (EACMS).

The management system could fall within one of the existing CIP cyber asset classifications. Based on our proposed language to the R1 part 1.1, the SDT only needs to add EACMS to R1 part 1.2 to resolve the zero trust model scenario.

Recommendation:

- Restore current CIP-005-6 R1.2 Requirements language and add “or EACMS”. The Requirements language could be such as:

“All External Routable Connectivity must be through an identified Electronic Access Point (EAP) or EACMS controlling communications to and from the BES Cyber System.”

Comment: If SCI is hosting a similar trust BCS then the SCI would be high watermarked to that trust level and should be exempt from R1.2. If the concern is transient execution then it would not make sense that the VCA within the BCS would be sharing the same resources as well.

Recommendation: If this is not a security concern, then in a similar trust environment, Management Systems should be excluded from R1.2

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

The proposed revision to CIP-005 R1.2 does not provide clarity related to “controlled communications.” If an entity permits needed communications, does that mean it is controlled? The requirement text starts with “Permit only needed…” which appears to make “controlled” unnecessary. Additionally, the term logical isolation is not defined and is subject to interpretation.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer No

Document Name

Comment

Comments: We believe there are more efficient methods to meet the SAR. Refer to the comments in QUESTION 1 regarding existing definitions.

The term “Management Interface” already exists in the inherent properties of a Cyber Asset in the manner in which a Cyber Asset connects to the network – i.e., copper, fiber, wireless, etc.… If the intent was to address access to a Cyber Asset, the existing language covers these controls in electronic access – ports and services and authentication (EACMS).

The management system could fall within one of the existing CIP cyber asset classifications. Based on our proposed language to the R1 part 1.1, the SDT only needs to add EACMS to R1 part 1.2 to resolve the zero trust model scenario.

Recommendation:

- Restore current CIP-005-6 R1.2 Requirements language and add “or EACMS”. The Requirements language could be such as:

“All External Routable Connectivity must be through an identified Electronic Access Point (EAP) or EACMS controlling communications to and from the BES Cyber System.”

Likes 0

Dislikes 0

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer No

Document Name

Comment

Reclamation recommends the virtualization requirements contain direct and detailed references to associated physical security requirements that protect and manage the equipment containing the virtual systems. Without this information, field employees could erroneously focus only on the logical protections.

Reclamation also recommends physical security requirements be connected to their associated virtualization requirements with direct and detailed references to clarify what is being protected.

Technical Guidance talks about the new term Management Interface being protected as described in CIP-005 R1 P1.2, but the redline for CIP-005 R1 P1.2 has no mention of the term Management Interface (only refers to Management Module). The Technical Guidance describes that Management Module will be addressed in CIP-005 R1.5, but there is not mention of Management Module in this Requirement.

Likes 0

Dislikes 0

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

ISO-NE generally agrees with the proposed changes. However, the requirement for anti-affinity rules for Management Systems appear to be overly burdensome and may outweigh any security benefit. We recommend allowing Management Systems to share memory and CPU with high-watermarked BES Cyber Systems as it still provides adequate security and eliminates the need for a physical host that would serve a single VM in many cases.

Additionally, as with the other proposed modifications, the “Applicable Systems” column should be reviewed for clarity, consistency and readability.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

RF does not agree with the proposed changes for the following reasons: As with other Standards and Requirements, a definition of logical isolation is required.

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed such that the entity first identifies needed communications, then applies control of the permitted communications. Suggested language for R1.2.2 - 1.2.2. Identify needed communications and control permitted communications to and from Management Interfaces and Management Systems, logically isolating all other communications.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No

Document Name	
Comment	
Although we agree with the proposed requirement, we are concerned with the lack of clarity in the examples provided in the Measures for R1.2. Specifically, we would encourage the SDT to consider replacing the first bullet with “Logically isolated out-of-band network infrastructure configuration (firewall, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, other Layer 2/Layer 3 controls, multi-tenant environment, or encryption).	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Request clarification of requirements (1.2.1, 1.2.2, 1.2.3) with applicable systems such as EACMS. Do these requirements (1.2.2, 1.2.3) apply to the “management interface” without “management systems”?	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	No

Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture. I have a request for additional information from the Standards Drafting Team to get clarity.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed suchthat the entity first identifies needed communications, then applies control of the permitted communications. Suggested language for R1.2.2 - 1.2.2. Identify needed communications and control permitted communications to and from Management Interfaces and Management Systems, logically isolating all other communications.	
Likes 0	

Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	No
Document Name	
Comment	

Best practices for vSphere suggest virtualizing vCenter (a Management System). However, for smaller entities who may only have a handful of Management Systems, requiring these systems to not share CPU and memory with other systems eliminates many of the benefits of virtualization and increases the complexity for no real tangible gain. This is compounded if the entity wants to implement best practices and have redundant Management Systems. Additionally, there are additional protections that are not accounted for by the proposed requirement, such as isolating the SCI from the internet or other controls that would mitigate such issues. See comments for question 19.

The language here creates a confusing scoping issue. The entity must look to three places to determine if a device must comply with the requirement, first the Applicable Systems column to find the "applicable system" (despite the fact the applicable system itself is not the device that needs to comply), the text of the requirement then to find which device actually needs to comply, and finally the definition Management System/Interface to see which devices meet that definition. Instead, the SDT should scope the Management System/Interfaces in the Applicable System column. That would allow the SDT to include logical isolation of Management Systems/Interfaces in CIP-005 R1.1 and isolation of BCS from Management System/Interfaces could be its own requirement part. For example, the Applicable Systems text could read, "Management Systems of SCI (and associated Management Modules) hosting High or Medium BCS or their associated: PCA; PACS; or EACMS".

Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Applicable system mentions "management modules of SCI". Requirements mention "Management system", "Management Interface". Those management reference three different definitions. Request clarification on the requirements (1.2.1,1.2.2,1.2.3) on management modules of SCI

With the new definition of EACMS (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of the logical isolation of BES Cyber Systems), why specify "EACMS that perform logical isolation for a High Impact BCS", its clear that and EACMS is a logical isolation.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

The added complexity of Part 1.2, the retirement of the defined term 'EAP' has expanded the scope from devices strictly residing in an ESP to additional network segments which were previously not in-scope with the requirement The appears to be some ambiguity of the additional compliance requirements and the new terms.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

Oklahoma Gas and Electric supports the comments provided by EEI.

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx

Comment

See attachment for comments.

Likes 0	
Dislikes 0	

Response

Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	

There are more efficient ways methods to meet the SAR. Existing deifnitions should be revisited. The management system will fall within one of the existing CIP cyber asset classifications.

As stated earlier, Basin would be in support of keeping the conceot of EAC and EACMS depending on how they define and write up EAC and EACMS.

Likes 0	
Dislikes 0	
Response	

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	

The proposed language in R1.2.2. and R1.2.3 seems to be contradictory given that R1.2.2 permits and R1.2.3 denies communications to and from Management Interfaces and Management Systems. CEHE suggests that the SDT consider clarifying the intention of the requirements.

Likes 0	
Dislikes 0	
Response	

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	

See MEC and BHE comments.

Likes 0	
Dislikes 0	
Response	

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

The proposed language in R1.2.2. and R1.2.3 seems to be contradictory given that R1.2.2 permits and R1.2.3 denies communications to and from Management Interfaces and Management Systems. SIGE suggests that the SDT consider clarifying the intention of the requirements.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	No
Document Name	

Comment

AZPS generally agrees with the proposed change to establish logical isolation requirements for Management Systems, Management Interfaces and associated SCI. We would like a clearer definition and understanding of what the term “logical isolation” means. Are the examples provided in the parenthesis, valid examples of logical isolation, ACL/VLAN/VXLAN/MPLS/VRF/multi-context, or multi-tenant environment.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP is concerned that the requirements containing the term logical isolation present a potential ambiguity for determining compliance. Logical isolation should be defined to ensure entities can achieve the performance-based requirement. AEP fully supports EEI’s suggestions, copied below for reference.

Specific Comments:

Requirement R1, Part R1.2

Please clarify how Requirement R1, Part R1.2 might apply to substation environments where no SCI exists.

1.2.1: The proposed definition of "Management System" lacks sufficient clarity (see our response to Question 1). We understand Management System to mean hypervisor. If this understanding is correct, the management system is what defines CPU/memory usage for its child VCAs. From this perspective, we request clarification on how management systems would restrict CPU/memory usage of other management systems and whether this is intended to be used for cloud-type services. To resolve this issue, the current language for this requirement should be clarified with additional explanation provided in the Technical Rationale.

1.2.2: AEP asks for clarification on why Management Modules have not been included in the language for this requirement, along with Management Interfaces and Management Systems. We note that Management Modules are included in the Applicability and Measures section but not in the Requirements. Please clarify whether this was intended and why or whether this was an oversight.

1.2.3: It appears that Part R1.2.2 already requires limiting the communication to Management Interfaces and Management Systems. Should this requirement be understood to mean that all communications to these Management Interfaces and Management Systems from BCS and their associated PCAs is to be denied? AEP requests clarification for this requirement.

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	No
Document Name	

Comment

As written, this standard appears to require that Management Interfaces be configured with logical isolation from the BCSs. It is unclear what security benefit this achieves. Management Interfaces in the same VLAN as BCSs would be as secure as the BCSs, therefore access to the Management Interface would be restricted even in that configuration. We would prefer to have the option of configuring Management Interfaces in the same VLAN as BCSs.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	No

Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Requirement R1.2 applies to EACMS that perform logical isolation for a High or Medium Impact BCS. EACMS could be a traditional firewall or a virtual firewall. R1.2.3 may cause confusion and prevent entities from communicating their EACMS (traditional firewall in this case) from within an ESP, such as BGP. Suggest clarifying that R1.2 is only applicable to virtual constructs, or R1.2.3 is only applicable to management access only.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No

Document Name	
Comment	
System should continue to follow security model of complete distrust. Only communication that is required must be allowed. This can only be established if rules are explicit including, Source, destination, Ports and Protocol. New application is very subjective and confusing. Industry is currently using Goose and still compliant, why change configuration and standards must be technology neutral.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We feel that a separate Part should be written in regards to SCI, leaving the existing CIP-005 Part 1.2 as currently written.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	

Comment	
FMPA supports Marty Hostler and Northern California Power Agency comments.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-005, R1, Part 1.2. PG&E does have concerns and supports the input provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
Permitting only “needed and controlled communications” is confusing. Controlled communications could be needed and needed communications should be controlled. We suggest the requirement be changed suchthat the entity first identifies needed communications, then applies control of the permitted communications. Suggested language for R1.2.2 - 1.2.2. Identify needed communications and control permitted communications to and from Management Interfaces and Management Systems, logically isolating all other communications.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the SRC.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb	

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 3.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

General Comment: The requirements containing the term logical isolation represent a potential ambiguity for determining entity compliance. Logical isolation should be defined to ensure entities can achieve the performance-based requirement. (see our comments within Question 1).

Specific Comments:

Requirement R1, Part R1.2

Please clarify how Requirement R1, Part R1.2 might apply to substation environments where no SCI exists?

1.2.1: The proposed definition of “Management System” lacks sufficient clarity (see our response to Question 1). We understand Management System to mean hypervisor. If this understanding is correct, the management system is what defines CPU/memory usage for its child VCAs. From this perspective, we request clarification on how management systems would restrict CPU/memory usage of other management systems and whether this is intended to be used for cloud type services. To resolve this issue, the current language for this requirement should be clarified with additional explanation provided in the Technical Rationale.

1.2.2: EEI asks for clarification on why Management Modules have not been included in the language for this requirement, along with Management Interfaces and Management Systems. We note that Management Modules are included in the Applicability and Measures section but not in the Requirements. Please clarify whether this was intended and why or whether this was an oversight.

1.2.3: It appears that 1.2.2 already requires limiting the communication to Management Interfaces and Management Systems. Should this requirement be understood to mean that all communications to these Management Interfaces and Management Systems from BCS and their associated PCAs is to be denied? EEI requests clarification for this requirement.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	
Comment	
NERC glossary term needed. The term 'logical isolation' is used in a range of different contexts across many industries. Is it similar to 'deny by default'?	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	No
Document Name	
Comment	
PNMR agrees with comments from Joshua Andersen, On Behalf of: Salt River Project, WECC, Segments 1, 3, 5, 6	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	No
Document Name	

Comment	
Request a better separation for Requirements between SCI and locally managed for non-SCI. By including EACMS there will be additional work required to segment the networks between the IRA and management networks and would bring into scope more of the IT network. Additionally, we propose this as a different definition for IRA: Authenticated access (a person/human) to the BCS from a VCA outside the logical isolation zone containing the BCS.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Please see comments in response to Question No. 2.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	No
Document Name	
Comment	
Conceptually, the SRC agrees with what the SDT is proposing; however, CIP-005, R1, Part 1.2 envisions the segmentation of the management plane. What if the management plane cannot be separated? There should be allowance for this possibility. **Recommendation:** Modify Part 1.2 as follows: **1.2.1** “Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per ***Cyber Asset*** capability.” **1.2.3** “Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per ***Cyber Asset*** capability.”	
Likes 0	
Dislikes 0	

Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Duke Energy generally agrees with the proposed modifications. However, the proposed applicability may be confusing. Is SCI hosting only EACMS subject to requirements beyond that which presently applies to physical EACMS?

Duke Energy in concerned that the inclusion of physical EACMS in the applicability of this requirement represents a significant expansion of scope. It appears that management interfaces of substation firewalls would go from having no specific network-based CIP requirements to being relevant for additional restrictions that would present a high management burden. It is unclear whether local ACLs on those management interfaces would be sufficient to meet the new requirement.

Additionally, the requirement for anti-affinity rules for Management Systems appear to be overly burdensome in relation to the purported security benefit – allowing them to share memory and CPU with high-watermarked BCS provides adequate security and eliminates the need for a physical host that would serve a single VM in many cases. System capability is inadequately defined in this context (for example, is a two-host cluster with one host in maintenance mode given a “capability” waiver for allowing a resident virtual management system to share the remaining active physical host with virtual BES Cyber Assets?).

Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern supports the SDT’s proposed direction in R1.2, and requests the SDT to consider the following with regard to the use of these two statements used throughout CIP-005:

1. “Permit only needed and controlled communications to and from…”

2. “Logically isolate all other communications…”

Here, the act of “permitting only needed and controlled communications” is also a form of “logical isolation.” We suggest the SDT consider the below proposed modifications for multiple requirements that carry this former language:

1. “Implement Logical Isolation to permit only needed and controlled communications to and from XYZ … and deny all other communications.”

Southern also reiterates that the requirements for logical isolation represent a potential compliance risk for applicable entities because the term is undefined, making the reliability objective unclear for the industry to ensure their processes will pass regulatory inspection. We encourage the SDT to define Logical Isolation to ensure entities can achieve the performance-based requirement.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC provides the following comments regarding CIP-005, requirement R1.2:

1. In the proposed revisions for CIP-005, for applicable systems, it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., “…hosting [] impact BCS and the BCS’s associated …..” or “….hosting [] impact BCS and the SCI’s associated…..”

2. In the applicable systems column, the reference to SCI includes an “or” and not an “and.” This creates uncertainty as to whether both “their associated EACMS or PACS” must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are “and” focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

3. In the defined terms, Management Modules are specifically excluded from SCI; however, the applicable systems column references Management Modules of SCI. This verbiage creates the potential for confusion and ambiguity relative to Management Modules. The following clarification is suggest to reduce the potential for ambiguity:

Management Modules supporting [or associated with] SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS

4. It is unclear why Management Modules are included in the applicable systems column of Requirement R1.2 when they are not specifically addressed in the requirements in the next column whereas other applicable systems are. Revision may be necessary to ensure clarity and consistent application and understanding.

5. Revise requirement 1.2.2. For clarity as follows:

Permit only controlled communications that are [necessary/needed] to and from Management Interfaces and Management Systems, logically isolating all other communications.

4. The SDT modified CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters. Does the proposed requirement fulfill the directive from FERC Order 791, paragraph 150? Please provide the basis for your response.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	
Comment	

MPC supports comments submitted by Duke Energy.

Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	Yes
Document Name	
Comment	

AEPCO is siging on to ACES comments.

Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	Yes
Document Name	

Comment	
The applicable system mentions “management modules of SCI”. Requirements mention “Management system”, “management Interface”. That management references three different definitions. Request clarification on the requirement (1.2.1, 1.2.2, and 1.2.3) on a management module of SCI. With the new definition of EACMS (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of logical isolation of BES Cyber Systems), why to specify “EACMS that perform logical isolation for a High Impact BCS”, it’s clear that and EACMS is logical isolation.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Victoria Mordi - Entergy - 3,7,9 - SERC

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	

Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE agrees that there should be CIP applicable Requirements and Parts for Management Systems, Management Interfaces, and associated SCI. Although not specifically related to virtualization, Texas RE recommends Management Modules should also apply to BCAs, PACS, and EACMS that are not on the SCI. Texas RE seeks clarification on whether management modules on current applicable BCAs, PACS, EACMS that are not on SCI are applicable to the CIP Requirements and Parts in the Applicable Systems column.

Likes 0	
Dislikes 0	

Response

4. The SDT modified CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters. Does the proposed requirement fulfill the directive from FERC Order 791, paragraph 150? Please provide the basis for your response.	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Please see comments in response to Question No. 2. As written, including PACS will be an issue because PACS are not required to be within a PSP and actually control the PSP.	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	

Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	No
Document Name	
Comment	
While it might fulfill the directive from FERC, it is unclear what technology would be used to accomplish this. Would we need to create IPSEC tunnels between switches on the same network but in different PSPs and have cabling traversing those PSPs? Or does the SDT believe something like IPv6 to be a valid way of complying with this requirements?	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI is concerned that the change that moved CIP-006 R1.10 to CIP-005 R1.3 has created some unintended reliability gaps that appear to exceed the scope of the Project 2016-02 SAR. In CIP-006-6, Requirement R1, Part 1.10 specific changes were made to satisfy FERC Order 791, paragraph 150 regarding access physical restrictions to cabling and other nonprogrammable communications components used for connection between appliable Cyber Assets within the same ESP. Among the applicable systems identified to satisfy this Commission-mandated change included “Medium Impact BES Cyber Systems at Control Centers and their associated PCA”. However, the new requirement in CIP-005 R1.3 does not duplicate this requirement and fails to specifically include language identifying Medium Impact BES Cyber Systems at Control Centers. EEI recommends the restoration of the CIP-006 Requirement R1, Part 1.10 in its entirety or modify CIP-005 to fully address the identified reliability gap.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb	
Answer	No
Document Name	
Comment	

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 4.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Exclusions have an undefined term. Proposed Requirements address some of the protections of a communication network without defining it.

Request removing specific technologies like encryption.

Request new wording on the exclusion of CIP-012 and time-sensitive protocols since Real-time Assessment and Real-time Monitoring are not clearly defined.

The proposed change isn’t in relation to the SAR. The requirement should have stayed in CIP-006, furthermore, the new requirement isn’t in tune with the old requirement.

Suggest removing any reference to “communications using protocol IEC TR-61850-90-5 R-GOOSE”, what about other similar protocols.

Suggest removing any reference to “CIP-012”.

Suggests stating the exclusion to *time-sensitive protection or control functions*, which is the common language.

Suggest removing any reference to “physical controls” as the concept of implementing confidentiality and integrity controls can include physical controls.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

We agree with the changes for CIP-005 R1 Part 1.3.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-005, R1, Part 1.3. PG&E does have concerns and supports the input provided by EEI.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerns on the definitions caused this no vote for this standard.

The “Physical controls that restrict access to the cabling and other nonprogrammable communication components,” should be moved to CIP-006 with all other physical security controls.

Request new wording on the exclusion of CIP-012 and time-sensitive protocols since Real-time Assessment and Real-time Monitoring are not clearly defined.

The exclusion for CIP-012 should be expanded to also exclude communication to a Control Center owned by others. The current language seems to require a GO with only a control room, to encrypt their communication to an LCC or ISO.

Suggest excluding voice communications as is done in CIP-012

Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	
FMPA supports Marty Hostler and Northern California Power Agency comments.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
The modified requirement covers all medium and high impact BES Cyber Systems. The former requirement's scope was limited to high BCS and medium impact BCS at Control Centers. This would require significant changes to BES facilities with medium impact BCS which are not Control Centers, such as large generation facilities which have disperse PSPs. This change is not in the scope of the SAR and should be updated such that the scope is limited to the prior version.	
Likes 0	
Dislikes 0	
Response	

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Remove the reference to encryption. This could be added to measures for this requirements

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

Applicability section is confusing. Too much compartmentalization of devices and non-industry standard definition are not needed. BCS definitions should be updated to address logical assets and apply high watermarking.

Current approach limits security with assumption that associated devices can be compromised externally, but BES impact must be considered if Cyber system is compromised and made unavailable.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AEPCO is signing on to ACES comments, please see below: The modified requirement covers all medium and high impact BES Cyber Systems. The former requirement's scope was limited to high BCS and medium impact BCS at Control Centers. This would require significant changes to BES facilities with medium impact BCS which are not Control Centers, such as large generation facilities which have disperse PSPs. This change is not in the scope of the SAR and should be updated such that the scope is limited to the prior version.	
Likes 0	
Dislikes 0	

Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP fully supports EEI's comment with the concern that the change of moving CIP-006 R1.10 to CIP-005 R1.3 has created some unintended reliability gaps that appear to exceed the scope of the Project 2016-02 SAR. As noted in EEI's comments, specific changes were made in CIP-006-6, Requirement R1, Part 1.10 to satisfy FERC Order 791, paragraph 150 regarding access physical restrictions to cabling and other nonprogrammable communications components used for connection between applicable Cyber Assets within the same ESP. Among the applicable systems identified to satisfy this, Commission mandated change included "Medium Impact BES Cyber Systems at Control Centers and their associated PCA". However, the new requirement in CIP-005 R1.3 does not duplicate this requirement and fails to specifically include language identifying Medium Impact BES Cyber Systems at Control Centers.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS would like to know if the amendments to CIP-005 R1.3 porting over from CIP-006 R1.10 exceed the scope of the SAR, due to the lack of the language to medium impact at control centers?	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by Duke Energy and submits the following comment for consideration:	

MPC requests a clarification on the intent of the changes to CIP-005 R1.3. The proposed language would require physical protections for data traversing communication links between two adjacent PSPs within a substation control yard with no virtualization present. This effectively extends CIP-006-6 R1, part 1.10 to medium impact BES Cyber Systems. Is this the intent of the drafting team? The SAR does not contain any language that would support this change when virtualization is not present.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

The proposed Requirement, R1 Part 1.3, states that the use of encryption or physical controls are acceptable; however, the Measures do not state that evidence may include proof of physical controls. The SDT needs to include evidence of physical controls in the Measures section, such as,

“Evidence may include, but is not limited to:

• architecture documents detailing the methods used to protect the confidentiality and integrity of the data (e.g., encryption), or

• documents detailing the physical control methods used to restrict access to the cabling and other nonprogrammable communication components.”

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

See MEC and BHE comments.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
The proposed Requirement, R1 Part 1.3, states that the use of encryption or physical controls are acceptable; however, the Measures do not state that evidence may include proof of physical controls. The SDT needs to include evidence of physical controls in the Measures section, such as, "Evidence may include, but is not limited to: • architecture documents detailing the methods used to protect the confidentiality and integrity of the data (e.g., encryption), or • documents detailing the physical control methods used to restrict access to the cabling and other nonprogrammable communication components."	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
As stated earlier, Basin would be in support of keeping the conceot of EAC and EACMS depending on how they define and write up EAC and EACMS.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

Oklahoma Gas and Electric supports the comments provided by EEI.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

“Physical controls” as used in the requirement is unclear. NIPSCO requests that the SDT provide clarity on what “physical controls” entail. Examples of such controls would be valuable. For example, is jacketed fiber a sufficient physical security control, and in what situation(s)?

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

The proposed change isn’t in relation to the SAR. The requirement should have stayed in CIP-006, furthermore, the new requirement isn’t in tune with the old requirement.

Suggest removing any reference to “communications using protocol IEC TR-61850-90-5 R-GOOSE”, in order to take into consideration other similar protocols?

Suggest removing any reference to “CIP-012”

Suggest stating the exclusion to *time-sensitive protection or control functions*, which is common language.

Suggest removing any reference to “physical controls” as the concept of implementing confidentiality and integrity controls can include physical controls.

Likes 0	
Dislikes 0	

Response

Victoria Mordi - Entergy - 3,7,9 - SERC

Answer	No
Document Name	

Comment

REDLINE: ‘R1 Part 1.3...Protect the data traversing communication links, where the logical isolation spans multiple Physical Security Perimeters, through the use of: confidentiality and integrity controls (such as encryption)...”Is one interpretation that we will have to encrypt between Medium and High? If “yes” to this, then Entergy response is to clarify the requirement further... Entergy is currently not in a position to encrypt from Medium to High... If “no”, then Entergy is in agreement with NERC proposal.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	No
Document Name	

Comment

CHPD supports the move of CIP-006 R1.10 to CIP-005, as it was not really a physical security requirement. The language still fulfills the directive of Order 791.

However, as with CIP-005 R1.1, the inclusion of PACS and EACMS hosted on SCI is not consistent with the SAR and should be removed. Additionally, the scope has been expanded to beyond Control Centers, which should be removed.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with the changes for CIP-005 R1 Part 1.3. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture. I have a request for additional information from the Standards Drafting Team to get clarity.	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No
Document Name	

Comment

Having added “where logical isolation spans multiple physical security perimters” excludes a lot of traffic. Not sure why this is limited to traffic that is logically isolated vs all traffic which appears to be the intent of the ferc order. It would be good to narrow the traffic down to traffic that is crossing network equipment managed by a third party, a carrier, or communication links shared with other entities.

We do not feel that the standard addresses the protection of the non programmable aspect of communication networks as currently written because of the wording “where logically spans…”

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

The requirement should have stayed in CIP-006, furthermore, the new requirement isn’t in tune with the old requirement.

Likes 0	

Dislikes 0

Response

Erin Green - Western Area Power Administration - 1,6

Answer No

Document Name

Comment

Support the comments of Barry Jones (WAPA).

Likes 0

Dislikes 0

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer No

Document Name

Comment

RF believes there should be a minimum level of encryption required to ensure that older, less secure methods of encryption are not used.

Likes 0

Dislikes 0

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer No

Document Name

Comment

Southern supports the modifications to CIP-006-6 R1.10 and moving it to CIP-005-8 R1.3 to continue to satisfy the Commission's directive in FERC Order 791 (paragraph 150.). Specifically, the deletion of CIP-006, Requirement R1, Subpart 1.10 and the development of a new requirement within CIP-005-8 (i.e., Requirement 1, Subpart 1.3) to protect "nonprogrammable" communication devices within networks that span multiple PSPs, per FERC Order 791, paragraph 150, *is achievable if simply relocating a requirement*. However, Southern questions the SDTs intent in removing medium impact BCS at Control Centers as an Applicable System, and replacing it with medium impact BCS connected to a network via a routable protocol. This alone has the potential to greatly increase the scope of the former CIP-006-6 R1.10 requirement, and the risk reduction or BES reliability benefit is not fully understood.

Additionally, Southern fails to see the need to add PACS and EACMS hosted on SCI, and the SCI hosting those PACS and EACMS, to the Applicable Systems column. Southern requests the SDT provide additional context into these additions from the former CIP-006-6 R1.10 requirement; specifically, is there commensurate increase in risk and probability for EACMS and PACS warranting this scope expansion? Is there a reliability benefit to "protect the data" traversing communication links between two or more PACS or EACMS assets residing on the same SCI if that SCI physically spans more than one PSP, but that does not apply when these are physical stand-alone assets? To now add EACMS and PACS data protections is an unexpected scope expansion, and the risk reduction or BES reliability benefit is not clearly understood. Under R1.3, the SDT appends the phrase "connected to a network via a routable protocol" for medium impact BCS, but does not also use this phrase for the high impact BCS, which it did use under R1.1. Is there a specific purpose for this omission here in R1.3? Additionally, the SDT appears to be inconsistently using the conjunctions "and" and "or" within the Applicable Systems column. For example – R1.1 uses "**AND** their associated:", but R1.2 uses "**OR** their associated:" and R1.3 uses both "and" and "or" when describing associated Cyber Assets as Applicable Systems. Is this inconsistency intentional?	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE agrees that the revisions to the requirement address some of the reliability concerns raised as an issue in FERC Order 791, but ISO-NE does not believe that the revisions fulfill the directive from paragraph 150. The term "communication networks" needs to be defined, but there has been no attempt to do so in the revisions.	
Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	

Comment

Consideration should be given to add "an equally effective logical protection" in the requirements which will allow for addtiional solutions to address the requirement.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

Reclamation recommends that Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and other BES Cyber Systems could be housed within virtual machines providing the same functionality residing locally on entity-owned computer hardware. Demarcation points of physically separated hardware and communication pathways between virtualized environments must be robust, redundant, and physically separated. Reclamation recommends virtual firewall appliances be used to segregate High/Medium/Low Impact systems in virtual environments. If virtual firewalls are used, mixed trust environments may not be an issue but hardware and supporting systems will need to be protected physically and electronically at the highest system impact level residing on the physical hardware.

Reclamation also recommends that with Standards working on a zero-trust model there needs to be a documented approval process above technical support staff to make changes and approve any trust relationships.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Comments: The proposed language to addresses CIP-006-6 R1.10, exceeds the SAR. There is a current exclusion for communications equipment and links between ESPs – which implies multiple physical locations. If the SDT intended to address the exclusions of discrete communications links between ESPs, then we suggest a revision to CIP-006-6 R1.10. If NERC is interested in addressing confidentiality and integrity between multiple ESPs (i.e., a super ESP), then we suggest a new SAR to add additional requirements.

Recommendation:

- Restore current CIP-005-6 R1.3 language to retain the EAP and revise to include EACMS. Requirement language could be “Utilize an EAP or EACMS, to require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.”

Suggest changing the Applicable Systems for CIP-005-6 R1.3 to:

“High Impact BES Cyber Systems and their associated:

- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

• PCA”

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: The proposed language to addresses CIP-006-6 R1.10, exceeds the SAR. There is a current exclusion for communications equipment and links between ESPs – which implies multiple physical locations. If the SDT intended to address the exclusions of discrete communications links between ESPs, then we suggest a revision to CIP-006-6 R1.10. If NERC is interested in addressing confidentiality and integrity between multiple ESPs (i.e., a super ESP), then we suggest a new SAR to add additional requirements.

Recommendation:

- Restore current CIP-005-6 R1.3 language to retain the EAP and revise to include EACMS. Requirement language could be “Utilize an EAP or EACMS, to require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.”

Suggest changing the Applicable Systems for CIP-005-6 R1.3 to:

“High Impact BES Cyber Systems and their associated:

- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

• PCA”

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

1. SRP in general, the inclusion of virtualization concepts with newly defined Applicable Systems makes the requirements harder to understand and identify what is truly applicable. SRP doesn’t like how all standards increased in size due to these additions. SRP would prefer to implement a way to account for virtualization without sweeping changes – similar to Low Impact. The attention given to virtualization feels over weighted compared to non-virtualized systems. This increases the burden on entities without virtualization to comb through the standards to find what is applicable.

2. SRP reads the rational to imply that the communications need to be encrypted if the communications link is provided by a 3rd party, however the verbiage of the standard excludes that detail. Is encryption required if the communications infrastructure is soley under the control of SRP?

3. Does SRP need to encrypt the communications to the multiple PSPs, or can we protect the links with a harden conduit between both PSPs – more of an explanation is needed. It mentions protect the data traversing communication links, where the logical isolation spans multiple PSPs.

4. SRP request the clarification on third party communications, and devices not within the PSP. Standard does not specifically call out third party communications. Standard is not specific in listing what equipment or types of equipment and what communication links are included.

5. SRP considers this requirement to be written for both Physical and Virtual environemnts.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Entities should have the flexibility to utilize emerging technologies to protect data in transit.

Likes 0	
Dislikes 0	

Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not generally agree with the proposed modifications. It is not clear how this impacts existing compliance postures for CIP-006 R1 for ESPs that span multiple PSPs. It appears there may be a significant scope expansion based on the new applicability as written to Medium BCS at Generation facilities, with limited reduction of risk. Duke Energy believes the proposed language to address CIP-006 R1.10 potentially exceeds the scope of this SAR.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	Yes
Document Name	
Comment	
Proposed CIP-005, Requirement R1, Part 1.3 partially addresses the reliability gap raised in FERC Order 791, paragraph 150; however, it does not define "communication networks," so that aspect remains outstanding. **Recommendation:** To address FERC's concern, define the term "communication networks."	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	

Answer	Yes
Document Name	

Comment

PJM signs on to the comments provided by the SRC.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Issue 1:

The intent of removing CIP-006 R1 Part 1.10 in favor of a single requirement to address this security objective of ensuring the confidentiality and integrity of data when moving across unprotected physical space is positive, however the Applicability of the Requirement parts differs. CIP-006 R1 Part 1.10 applies to Control Centers only, and this change will force additional locations to be secured that are not currently required.

Issue 2:

Tacoma Power requests the SDT provide clarification on their intent for using the language “confidentiality and integrity controls (such as encryption)” rather than the general language of “encryption”. It would be helpful if the SDT would provide guidance on what type of evidence can be used to meet the confidentiality and the integrity in the Measures column for this Requirement. For example, an entity may choose to use an IPSEC Site-to-Site VPN to secure communications. The IPSEC VPNs are configured to use IKE v2 with AES256 encryption to provide confidentiality and certificates for authentication to provide integrity for the link. Is this the type of evidence the SDT is looking for to meet the requirement, or is simply providing evidence the link is encrypted sufficient to meet the SDT’s intent for using the confidentiality and integrity controls language? Suggest including specific technology examples within the Implementation Guidance, much like was presented at the March 3, 2021 Webinar.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC agrees that the requirement fulfills the directive and respectfully suggests the following clarifications:

1. In the applicable systems column, the reference to SCI includes an “or” and not an “and.” This creates uncertainty as to whether both “their associated EACMS or PACS” must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are “and” focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

2. Clarification of the included exclusions is recommended as follows:

…excluding data being transmitted between Control Centers that is subject to CIP-012 and time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

We recognize that the SDT has realigned the requirement to protect nonprogrammable communication components from CIP-006 R1 to CIP-005 R1. As CIP-006 R1 previously addressed Order 791 Paragraph 150, we feel CIP-005 R1 continues to address the identified gap.

Likes 0	
Dislikes 0	

Response

Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6

Answer	Yes
Document Name	

Comment

Change follows FERC Order 791, however, reference to the CIP-012 standard and the addition of a specific protocol in the requirements area should be removed and placed into the measures area.

Likes 0	

Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
The proposed requirement appears to meet the directive in FERC Order 791, paragraph 150. However, the proposed applicability of this requirement significantly expands the scope from CIP-006 R1.10 that focuses on Control Centers to high/medium BES Cyber Systems, PCAs, PACS, and EACMS. This revision appears to be beyond the scope of the SDT's SAR.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE does not have comments on this question.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	
Document Name	

Comment

Please see comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

5. The SDT modified CIP-005 Requirement R2 to ensure remote access management requirements align with the new and revised virtualization terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Clarify the definition of "system to system" in Parts 2.4 and 2.5 to provide consistent application of the standard.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

1. As SRP reads, R2.1: “Ensure…” should be replaced with strong verbiage. R2.2: “Protect the confidentiality and integrity…” appears to provide flexibility, it will likely result in entities seeking and following the opinion of auditors on what is sufficient. SRP would prefer 2.2 be the first requirement in the R2 section, then 2.1 and 2.3.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: In order to accommodate the SDT language for these requirements, the definition of IRA could be revised per our recommendations in Question 1 to include routable connectivity for the initiation of Interactive Remote Access.

Recommendations:

- Retain the current CIP-005-6 R2 language and revise the Applicable Systems to change from Medium Impact with ERC to Medium Impact with IRA.
- Retain the current CIP-005-6 R3 language for Applicable Systems.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

The proposed definition and requirements decouple ERC as a qualifier for IRA and imposes additional requirements on systems that were previously out of scope. This prevents backwards compatibility for entities with serial connections to medium impact BCS at substations and generation facilities. The requirement was modified to address conversion from IP to serial protocol conversion at a substation or generating facility due to the perceived risk of the routable communications. However, the changes adversely impact entities that use the “500 mile serial cable” for communications. How does an entity protect confidentiality and integrity of communications on a serial link that transverses through an asset boundary? The proposed revisions ultimately require the conversion of substations/facilities with serial connections to BCS with ERC in order to meet IRA requirements in CIP-005 R2.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Comments: In order to accommodate the SDT language for these requirements, the definition of IRA could be revised per our recommendations in Question 1 to include routable connectivity for the initiation of Interactive Remote Access.

Recommendations:

- Retain the current CIP-005-6 R2 language and revise the Applicable Systems to change from Medium Impact with ERC to Medium Impact with IRA.

Retain the current CIP-005-6 R3 language for Applicable Systems.

Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
Document Name	
Comment	
An entity may find the wording confusing. It could be read as only communication to another Intermediate System is permitted. In addition, in this case, recommend changing the term “Intermediate System” to “EACMS used to restrict IRA”.	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	No
Document Name	
Comment	
The proposed language greatly expands scope of this requirement by adding PACS and EACMS, which were not previously in scope.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
For CIP-005 Requirement R2.1, ISO-NE recommends the replacement of the word “ensure” as this represents internal control language and is inconsistent with all other requirements. ISO-NE suggests the following replacement language: “For all IRA, utilize an Intermediate System (IS).”	

For CIP-005 Requirement R2.2, ISO-NE recommends removal of the cross-reference to another Part of the same requirement in the Applicable Systems, “Intermediate Systems used to access applicable systems of Part 2.1.” This approach deviates from other CIP “Applicable Systems” columns and requires a reader to refer to other requirements for scope. ISO-NE suggests either including the CIP-005 Part 2.2 requirements in the CIP-005 Part 2.1 requirements, or adjusting CIP-005 Part 2.2 to state “Intermediate Systems used for IRA.”

For CIP-005 Requirement R2.3, ISO-NE recommends removal of the cross-reference to another Part of the same requirement in the applicable systems, “Intermediate Systems used to access applicable systems of Part 2.1.” This approach deviates from other CIP “Applicable Systems” columns and requires a reader to refer to other requirements for scope. ISO-NE recommends adjusting CIP-005 Part 2.3 to state “Intermediate Systems used for IRA.”

Likes 0

Dislikes 0

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0

Dislikes 0

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern does not support the proposed changes to R2 and requests that the SDT consider the following comments:

• Southern requests that the SDT consider that the R2.1 requirement, as currently proposed, (1) adds further scope expansion from previous versions, and (2) reintroduces again the concept of the “Hall of Mirrors” where the object of the requirement (an EACMS-Intermediate System) is also an Applicable System (EACMS) where the object must apply the requirement to itself.

o In the first case, PACS assets have historically not been required to have an EACMS-Intermediate System regulate remote access to them; here PACS hosted on SCI have been added as an Applicable System, which now would require an entity implement an EACMS-IS for remote access to PACS assets hosted on SCI, and the IRA definition has been expanded to now make IRA applicable to PACS assets hosted on SCI because IRA is no longer tied to the outer boundary of an “ESP”.

o In the second case, the Applicable Systems column includes EACMS hosted on SCI, which now requires that IRA to an EACMS go through an Intermediate System; however, the Intermediate System is also an EACMS and IRA to it would therefore require another Intermediate System in front of it, and so on and so forth.

o However, a review of the revised definition of EACMS states:

 Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of **the logical isolation of BES Cyber Systems.** This includes Intermediate Systems.

 This definition of an EACMS explicity excludes itself from performing electronic access controls (IRA) or electronic access monitoring for PACS assets or other EACMS assets, whether hosted on SCI or not, and rather only includes that performance for the “***logical isolation*** of BES Cyber Systems”, and not PACS, other EACMS, or the BES Cyber Systems themselves.

• It is also not explicitly clear what is meant by the term “from outside of the asset containing the system being accessed” from the IRA definition. Southern recommends the SDT provides clarification on this specificity in defining IRA that appears to make any communication from outside of the “asset” (little “a”, Facility) where the system being accessed “resides” as now being IRA. This seems ot be a result of the concepts of losing the outer boundary of an ESP such that the definition of “remote” becomes very broad. As a result, for those entities that do retain ESPs as a form of Logical Isolation, this significantly complicates inter-ESP communication that spans multiple “assets” or Facilities.

• Under Requirement R2.6.1, the requirement is written in a way that could be interpreted to mean that all Intermediate Systems must be virtualized and therefore must, in every case, only “share CPU and memory with other Intermediate Systems and their associated SCI.” Southern requests the SDT consider the addition of the following phrase to the requirement as follows: “Restrict Intermediate Systems ***hosted on SCI*** to only share CPU and memory with other Intermediate Systems and their associated SCI.”

o Additionally, the R2.6.1 language confirms the interpretation that Intermediate Systems hosted on SCI and associated with any of the Applicable Systems from Part 2.1 cannot share virtual space or Management Systems with BES Cyber Systems or non-CIP assets, and therefore must be stand-alone systems. A utility is then required to have at least three separate sets of hardware/management systems: one for medium and high BCS, one for IS, and one for associated PACS and EACMS hosted on SCI (and more if using virtualization for non-CIP/exempt cyber assets and/or separating medium impact and high impact assets from a risk-based perspective). This seems to disincentivize the use of, and achievement of better security offered by, virtualized systems and architectures.

• The Technical Rationale for CIP-005-8 mentions that this is now an objective-based requirement, but that outdated encryption methods or protocols would not meet the objective. Who decides what encryption methods or protocols are “outdated” and thus would be non-compliant? Can a list of these be provided by NERC and the Regions? Can the SDT remove this from the TR and potentially allow common sense to apply to appropriate security and encryption protocols between entities and auditors?

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

RF does not agree with the proposed changes for the following reasons:

A significant concern is that an entity could implement logical isolation using only a host-based firewall and essential systems could be directly connected to the internet – a side effect breaking the definition of External Routable Connectivity and enabling entities to bypass many now-required protections.

With each system becoming its own ESP (zero trust) – mixing of CIP and non-CIP network traffic is permitted and could lead to issues regarding secure communications if implemented policies are not closely scrutinized and exceptional care taken to maintain and control policies on each individual Cyber Asset.

As written and presented, there is a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication, but have not adequately enforced protections to ensure that the ports are not used by malicious actors – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to ensure validity of communications to Applicable Systems.

Logical Isolation is not defined, leading to diverse definitions between the entities and regions.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

R2.1: The Intermediate System is an EACMS. Adding associated EACMS to the Applicable Systems creates an EACMS for an EACMS situation. There is no need for this requirement to be applicable to associated PACS or EACMS. The Intermediate System is designed to protect IRA sessions to logically isolated systems. If any PACS or EACMS are inside the logical isolations, then those PACS or EACMS are PCAs. We recommend removing “PACS or EACMS” from the Applicable Systems for both SCI and Management Modules.

R2.2: We understand the concept of the requirement as currently written, “ For all IRA sessions, utilize encryption that terminates at the Intermediate System.” The revised language “between the client and the Intermediate System” is not clear. Either clarify or define “the client” in the requirement or revert back to the current language.

R2.6: Is the intent to require any virtualized Intermediate System(s) to be hosted on SCI that does not contain virtual BCS, EACMS, PACS or PCAs? Please clarify the intent.

R2.6.2 seems duplicative of R1.1. R2 requires Intermediate Systems to be used to access logically isolated applicable systems. R1.1 requires that we identify needed communications. If the communications between the Intermediate Systems is needed and controlled into the logically isolated systems, then R2.6.2 is redundant and covered by R1.1. Please clarify the SDT intent for R2.6.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	
Comment	

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	
Response	

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	
Comment	

Could you please specify the kind of access you are referring to for IRA? For example, we have operators that will issue commands to close or open a breaker, start or shutdown a Turbine generating unit. But they don't have access to configure or change the configuration of the asset. In that case is that consider IRA ?

Our understanding is that the "User-initiated access by a person employing a remote access client" you are referring to, is basically **for configuration changes** from outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed.

Proposed definition:

User-initiated access by a person employing a remote access client from outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed; **excluding control functions** (e.g. access for issuing commands)

Likes 0	
Dislikes 0	
Response	

Ryan Olson - Portland General Electric Co. - 5

Answer	No
Document Name	
Comment	

Portland General Electric Company supports the comments provided by EEI for this survey question

Likes 0	

Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No
Document Name	

Comment

the standard requires that an entity must use an IS to access and EACMS but and IS is an EACMS so do you need and IS to access and IS? This comment is based on the interpretation by some SMEs that CIP-005 R2.1 includes with IRA including the VCA hosted by them (discussed below).

In requirement 2.1 for:

SCI with IRA hosting High or Medium Impact BCS or their associated:

PCA

PACS; or

EACMS

For R2.1 It is not clear if EACMS and PACS on SCI is applicable if there is no High or Medium Impact BCS on the same SCI. Some SMEs read that EACMS and PACS are only applicable if High or Medium Impact BCS are on the same SCI; other SMEs read the applicability to be associated EACMS and PACS on SCI, regardless of whether the High or Medium Impact BCS are virtual. A third way to interpret the applicability is that SCI with IRA hosting high or medium impact BCS or associated PCA, PACS or EACMS must have an intermediates system just to access the manament system. It’s unclear what the applicable systems are.

For CIP-005 R2 and others, where the intent may be to protect the SCI or have the SCI be the applicable system, it might be better to write like this:

SCI with IRA hosting:

High or Medium Impact BCS or their associated;

PCA;

PACS; or

EACMS

The above would make it clear that the applicable system is the SCI.

Likes 0	

Dislikes 0

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer No

Document Name

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer No

Document Name

Comment

As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture. I have a request for additional information from the Standards Drafting Team to get clarity.

Likes 0

Dislikes 0

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer No

Document Name

Comment

R2.1: The Intermediate System is an EACMS. Adding associated EACMS to the Applicable Systems creates an EACMS for an EACMS situation. There is no need for this requirement to be applicable to associated PACS or EACMS. The Intermediate System is designed to protect IRA sessions to logically isolated systems. If any PACS or EACMS are inside the logical isolations, then those PACS or EACMS are PCAs. We recommend removing “PACSor EACMS” from the Applicable Systems for both SCI and Management Modules.

R2.2: We understand the concept of the requirement as currently written, “For all IRA sessions, utilize encryption that terminates at the Intermediate System”. The revised language “between the client and the Intermediate System” is not clear. Either clarify or define “the client” in the requirement or revert back to the current language.

R2.6: Is the intent to require any virtualized Intermediate System(s) to be hosted on SCI that does not contain virtual BCS, EACMS, PACS or PCAs? Please clarify the intent.

R2.6.2 seems duplicative of R1.1. R2 requires Intermediate Systems to be used to access logically isolated applicable systems. R1.1 requires that we identify needed communications. If the communications between the IS is needed and controlled into the logically isolated systems, then R2.6.2 is redundant and covered by R1.1. Please clarify SDT intent for R2.6

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	No
Document Name	

Comment

CHPD does not agree with the CPU and memory isolation requirements. In particular, it prevents other potential mitigations, such as non-persistent Intermediate Systems where malware would be unable to gain a foothold, and unduly increases the cost of virtualization. See comments for question 19.

“(e.g., encryption)” in CIP-005 R2.2 should be moved to Measures.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Request clarification on R2.1 “ensure.” The requirement says “Ensure that IRA is through an Intermediate System.”

Request clarification on the definition of SCI (including Management Systems) and the column applicable systems, in requirement 2.1 Management Modules

Suggest not to include PACS and EACMS in the scope in the context of SCI as this requirement doesn't exist for a PACS and EACMS not on a SCI.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Additional clarity is needed on the new terms to see how this requirement affects an entity's facility that contain Medium Impact BCS.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	

Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
The definition of IRA would need to be reviesed to include routable connectivity for the initation of Interactive Remote Access.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree with the proposed changes to CIP-005 Requirement R2 due to the proposed IRA definition. Please see response to Question 1 for additional details.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	

SIGE does not agree with the proposed changes to CIP-005 Requirement R2 due to the proposed IRA definition. Please see response to Question 1 for additional details.

Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	

AEP is concerned that proposed changes to CIP-005 Requirement R2 may have created some unintended gaps in how the requirements may be audited and seeks additional clarification. AEP fully supports EEI's suggestions, copied below for reference.

Part 2.1: Requirements do not specify that the Intermediate Systems (IS) must be logically separated from the system being accessed. The current IS definition states that it must be located outside the ESP. The Technical Rationale for the IS definition states that placement of IS has been moved to R2. AEP seeks clarification on how this is addressed within Requirement R2.

Part 2.2: The proposed IRA definition states that IRA shall be from outside the logical isolation of the system being accessed. R2, Part 2.2 requires that IRA between client and IS must be protected. Assuming the client is the initiating device, there must be logical separation between client and IS. Considering this and what was previously required, separation was required between IS and BCA (i.e., "IS must be outside ESP"). AEP's concern with R2, Part 2.2 is that it is no longer clear if that level of isolation is still required. The existing requirement should be clarified to address what is required.

- Clarification is needed on the change from "encryption that terminates at an intermediate system" to "between client and the IS". It is not clear where encryption is required. Diagrams in the Technical Rationale would be useful to ensure that entities understand what is expected.
- We also note that the Technical Rationale states that R2, Part 2.2 is now objective-based and the requirement now "prevents outdated encryption methods from being used that no longer meet the objective." (CIP-005-8 Technical Rationale, R2, Part 2.2, page 10). Clarification is needed on who makes this determination and how this would be determined.

Part 2.6: AEP also suggests to add Applicable Systems from Part 2.1 to Part 2.6 instead of just referencing it.

- Part 2.6.1: Is this intended to separate IS from exempt cyber assets, meaning IS cannot be hosted by Management Systems shared with non-CIP systems? This also prevents IS from being hosted by Management Systems containing BCS. The result is that, in a virtualized environment, a utility requires three separate sets of hardware/management systems: one for medium and high BCS, one for IS, and one for non-CIP/exempt cyber assets. Can IS be hosted on SCI with non-CIP systems? Again, the "IS" definition in the glossary indicates IS placement is handled in CIP-005 R2 but that detail is not included here.

- Part 2.6.2: AEP is concerned that this requirement may be duplicative of Requirement R1, Part 1.1. In Part 1.1, it already requires that EACMS "Permit only needed and controlled communications to and from applicable systems" and the IS definition indicates it is a "type of EACMS". For these reasons, Clarification is needed on why R2, Part 2.6.2 is not duplicative to R1, Part 1.1.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AEPCO is signing on to ACES comments, please see below:

ACES does not agree with the language used in requirement R2.2. "Client" is a vague and an undefined term. We suggest:

Protect the confidentiality and integrity (e.g., encryption) of IRA between the remote host and the Intermediate System.

ACES does not agree with the language used in R2.6.2 as it is redundant to R1.1 and not necessary. If implemented, any communications with Applicable Systems in part 1.1 would already be permitted, controlled, and documented, which would include IRA, and make R2.6.2 unnecessary. If the scope of R1.1 does not include all of R2.1, updating the scope of R1.1 would suffice.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

CIP-005, R2.2 does not clearly define what a “client” would be in reference to encryption between the client and the Intermediate System. Additional clarity is necessary to ensure consistent application of the proposed Standard.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren generally agrees with EEI's comments with some added suggestions. We suggest that the SDT include examples of remote access that include a virtualized desktop environment. We also suggest that the IRA definition should say you cannot have IRA from another cyber asset.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

“Ensure that authorized IRA is through an Intermediate System. “ – Can we communicate through the firewall? Previous standard was accurate. New standard is subjective and will create confusion.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

The term “ensure” is unclear. How will this be interpreted by regions and auditors? This needs to be clarified

Likes 0

Dislikes 0

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0

Dislikes 0

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	No
Document Name	

Comment

R2.2 and 2.3: With the revised definition, it is unclear if Intermediate System, defined as “An Electronic Access Control or Monitoring System that is used to restrict Interactive Remote Access”, is referring to a jump host or an authentication system. Based on the language used, encryption is only required during the authentication phase.

R2.4: The language states that a method for determining active vendor remote sessions is required. However, the measures appear to be primarily focusing on logging of access while ignoring real time access. Is the intent to log, or is the intent to be able to identify active sessions. Intent and language in the requirement is unclear.

Likes 0

Dislikes 0

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

ACES does not agree with the language used in requirement R2.2. "Client" is a vague and an undefined term. We suggest:

Protect the confidentiality and integrity (e.g., encryption) of IRA between the remote host and the Intermediate System.

ACES does not agree with the language used in R2.6.2 as it is redundant to R1.1 and not necessary. If implemented, any communications with Applicable Systems in part 1.1 would already be permitted, controlled, and documented, which would include IRA, and make R2.6.2 unnecessary. If the scope of R1.1 does not include all of R2.1, updating the scope of R1.1 would suffice.

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer	No
Document Name	

Comment

FMPA supports Marty Hostler and Northern California Power Agency comments.

Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question.

Likes 0	
Dislikes 0	

Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
DTE sees the applicability for R2, as described in the R2 description, to be inconsistent and potentially confusing and recommends that the applicability, "For all remote access that does not originate from applicable systems in Requirement R1 Part 1.1 or Part 1.2.2, excluding Dial-up Connectivity and TCAs", be moved to the "Applicable Systems" section in some manner to avoid this confusion.	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP offers the following comment for the SDT consideration for Question 5: Recommend the SDT consider R2.6 be written in the definition, or considered in CIP-002.	
Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-005, R2. PG&E does have concerns and supports the input provided by EEI.

Likes 0

Dislikes 0

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

R2.1: The Intermediate System is an EACMS. Adding associated EACMS to the Applicable Systems creates an EACMS for an EACMS situation. There is no need for this requirement to be applicable to associated PACS or EACMS. The Intermediate System is designed to protect IRA sessions to logically isolated systems. If any PACS or EACMS are inside the logical isolations, then those PACS or EACMS are PCAs. We recommend removing “PACSor EACMS” from the Applicable Systems for both SCI and Management Modules.

R2.2: We understand the concept of the requirement as currently written, “For all IRA sessions, utilize encryption that terminates at the Intermediate System”. The revised language “between the client and the Intermediate System” is not clear. Either clarify or define “the client” in the requirement or revert back to the current language.

R2.6: Is the intent to require any virtualized Intermediate System(s) to be hosted on SCI that does not contain virtual BCS, EACMS, PACS or PCAs? Please clarify the intent.

R2.6.2 seems duplicative of R1.1. R2 requires Intermediate Systems to be used to access logically isolated applicable systems. R1.1 requires that we identify needed communications. If the communications between the IS is needed and controlled into the logically isolated systems, then R2.6.2 is redundant and covered by R1.1. Please clarify SDT intent for R2.6

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification on R2.1 “ensure.” The requirement says “Ensure that IRA is through an Intermediate System.”

Request clarification on R2.1 “ensure.” The requirement says “Ensure that IRA is through an Intermediate System.”

Request clarification on the definition of SCI (including Management Systems) and the column applicable systems, in requirement 2.1 Management Modules.

Suggest not to include PACS and EACMS into the scope in the context of SCI as this requirement doesn’t exist for a PACS and EACMS not on an SCI.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 5.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Requirement R2

2.1: Requirements do not specify that the Intermediate Systems (IS) must be logically separated from the system being accessed. The current IS definition states that it must be located outside the ESP. The Technical Rationale for the IS definition states that placement of IS has been moved to R2. EEI seeks clarification on how this is addressed within Requirement R2.

2.2: The proposed IRA definition states that IRA shall be from outside the logical isolation of the system being accessed. R2, Part 2.2 requires that IRA between client and IS must be protected. Assuming the client is the initiating device, there must be logical separation between client and IS. Considering this and what was previously required, separation was required between IS and BCA (i.e., “IS must be outside ESP”). EEI’s concern with R2, Part 2.2 is that it is no longer clear if that level of isolation is still required. The existing requirement should be clarified to address what is required.

EEI also seek clarification on the change from “encryption that terminates at an intermediate system” to “between client and the IS”. It is not clear where encryption is required. Diagrams in the Technical Rationale would be useful to ensure that entities understand what is expected.

We also note that the Technical Rationale states that R2, Part 2.2 is now objective-based and the requirement “prevents outdated encryption methods from being used that no longer meet the objective.” (CIP-005-8 Technical Rational, R2, Part 2.2, page 10). EEI requests clarification on who makes this determination and how this would be determined.

2.6.1: Is this intended to separate IS from exempt cyber assets, meaning IS cannot be hosted by management systems shared with non-CIP systems? This also prevents IS from being hosted by management systems containing BCS. The result is that, in a virtualized environment, a utility requires three separate sets of hardware/management systems: one for medium and high BCS, one for IS, and one for non-CIP/exempt cyber assets. Can IS be hosted on SCI with non-CIP systems? Again, the “IS” definition in the glossary indicates IS placement is handled in CIP-005 R2 but that detail is not included here.

2.6.2: EEI is concerned that this requirement may be duplicative of Requirement R1, Part 1.1. In R1, Part 1.1 it already requires that EACMS “Permit only needed and controlled communications to and from applicable systems” and the IS definition indicates it is a “type of EACMS”. For these reasons, EEI requests clarification why R2, Part 2.6.2 is not duplicative to R1, Part 1.1.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - Trevor Tidwell - 1,3

Answer	No
Document Name	

Comment

In R2 there is a Hall of Mirrors effect. In R2.1 it appears the EACMS on SCI needs to have IRA through an Intermediate System, but an Intermediate System itself is by definition an EACMS. So if I have my Intermediate System on SCI then does that Intermediate System which is a EACMS on SCI also need another Intermediate System to perform IRA?

We have a concern about R2.6. Many multifactor authentication systems reside on the domain controller. The Multifactor authentication is part of the Intermediate System. The concern is restricting the sharing of CPU and memory. These domain controllers may also be EACMS for other devices. Can we restrict the sharing of CPU and memory to other in scope CIP devices to allow more flexibility in architecture?

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	
Comment	
Request clarification on R2.1 “ensure.” The requirement says “Ensure that IRA is through an Intermediate System.”	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes that as presently drafted, CIP-005 R2 and CIP-005 R3 conflict with one another. Please see our explanation and recommendations for resolving this problem in our response to Question 19.	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	No
Document Name	

Comment

We don't agree with replacing ERC with IRA, as it will bring into compliance more devices that were previously excluded. Additionally, we recommend that R2.4 – 2.5 are updated with the same exclusion as R1.3 for Real-time Assessment and real-time monitoring data. We do not believe ICCP protocol should be considered vendor system-to-system remote access. Our EMS system does not allow modifications through the ICCP protocol, thus there is no "access".

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

The standard should contemplate the use of encryption and multifactor between the Intermediate System and the Cyber Assets within the ESP. As written, it appears to prohibit that.

ERCOT suggests that the Part 2.2 example should be in the measure.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Part 2.6.2 security objective appears to already be addressed in Part 1.1.	
Likes 0	

Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the proposed modifications, but has identified concerns with the impact of anti-affinity rules as described in the general comments below.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Reclamation recommends having a documented process for approving vendor remote access sessions through a change control board.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes this effectively expands the scope of the control by including serial only devices that allow interactive remote access via a serial to Ethernet converter. Guidance needs to make clear how an entity would comply with requirements intended for Ethernet protocols when using interactive remote access over serial connections.	
Likes 0	

Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

GSOC provides the following comments regarding the proposed revisions to CIP-005, requirement R2:

3. In the applicable systems column, the reference to SCI includes an “or” and not an “and.” This creates uncertainty as to whether both “their associated EACMS or PACS” must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are “and” focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

4. In the applicable systems column, ERC has been struck with respect to Medium Impact BCS and IRA or vendor remote access has been added. This is different from other areas where IRA has been added to a similar requirement and ERC has been retained and vice versa. While it is understood that such scoping can better tailor the requirements, inconsistent application and use of scoping verbiage can lead to ambiguity and confusion. For this reason, review and use of consistent scoping verbiage is recommended.

5. In the defined terms, Management Modules are specifically excluded from SCI; however, the applicable systems column in R2 and R3 references Management Modules of SCI. This verbiage creates the potential for confusion and ambiguity relative to Management Modules. The following clarification is suggest to reduce the potential for ambiguity:

Management Modules supporting [or associated with] SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS

6. The intent and expectations of requirement R2.1 is unclear. As revised, the new requirement could be construed as allowing the Intermediate System to acts as a pass-through or flow-through device that is not contributing to the security controls applied to IRA. Suggest clarification through the proposed revisions below:

Ensure that IRA is [implemented/controlled] through an Intermediate System.

7. CIP-004 does not address the authorization of electronic access to Management Modules; however, requirements in Requirement R2.1 hint that there are expectations and obligations associated with access to these assets. This should be clarified.

8. In requirement R2.6, the following revision is recommended for clarity:

2.6.2. Permit only controlled communications that are [needed/necessary] between Intermediate Systems and applicable systems of Part 2.1.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Tacoma Power requests clarification from the SDT regarding “confidentiality and integrity” controls and what encryption methodologies would serve the Requirement. This clarification could be contained in the CIP-005 Implementation Guidance describing message integrity provided by application layer encryption like HTTPS & TLS.	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	Yes
Document Name	
Comment	
For purposes of our response to question 5, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO and PJM.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon is aligning with EEI in response to this question.

Likes 0

Dislikes 0

Response

Cynthia Lee - Exelon - 5

Answer

Document Name

Comment

Exelon is aligning with EEI in response to this question.

Likes 0

Dislikes 0

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer

Document Name

Comment

Please see comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

6. The SDT revised CIP-007 Requirement R1 Part 1.1 to shift the security objective from logical network accessible ports to services. The proposed revisions require Responsible Entities to enable only network accessible services that have been determined to be needed by the Responsible Entity. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO signs on in support of SRC.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization

Answer	No
Document Name	

Comment

As written, CIP-007, R1, Part 1.1 continues to reference both ports and services:

- Requirement: “Enable only network accessible services that have been determined to be needed…, or the logical network accessible *ports* if unable to determine service, including *port* ranges where needed to handle dynamic *ports*) per system capability”
- Measure: “Documentation of the need for all enabled *ports*.”

Recommendation: If the intent is to focus on services only, the SDT should clarify this in non-ambigous terms; i.e. indicate entities will be audited on “**services only**” (as opposed to “*ports and* services”).

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

Please see comments submitted by the ISO/RTO Council Standards Review Committee.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST believes proposed changes beyond those needed for conformance:

Have little or nothing to do with virtualization,

Are unlikely to improve anyone’s cyber security posture,

Are outside the scope of the original 2016 SAR,

Are not addressed in any relevant FERC Order, and

Would be an unnecessary and unwelcome distraction for entities trying to adjust their CIP programs and documentation to accommodate new virtualization-related requirements.

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	No
Document Name	
Comment	
PNMR expresses support of comments by Joshua Andersen, On Behalf of: Salt River Project, WECC, Segments 1, 3, 5, 6	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
What is the value of removing ports if the phrase “(or logical ports)” is added every time services is used?	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	

Answer	No
Document Name	

Comment

General comment on CIP-007. Request consistent use of “system hardening.” We concerned that the label “system hardening” is used differently in the R3.1 Measures and with Transient Cyber Assets.

Request clarification of “services” – entity may need to map their BES Cyber Assets to Applicable Systems.

Suggest reviewing the Requirements column for requirements 1.1 and 1.3, the objective is the same, yet the text isn’t. It should have the same level of detail.

Suggest reviewing the Applicable Systems of CIP-007 should include Management Systems.

Suggest not to include PACS and EACMS into the scope in the context of SCI as this requirement doesn’t exist for a PACS and EACMS, not on an SCI. SAR is for including the virilization concepts not to add additional controls.

Suggest reviewing the Applicable Systems of CIP-007 associated with management modules. The current language only refers to Management Modules of SCI hosting what about the management module of a BCA? Management Modules of SCI hosting would have more controls than Management Modules of BCA.

Request clarification on the term system (cybersecurity patches for systems), the objective is for the system to be patched or for the cyber asset composing the system to be patched?

Request clarification on the term system capability (Log security events, per system capability), logging from one cyber asset would be enough to comply with the requirement?

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by SRC and requests additional clarity on the use of the term “enable”. Is the term intended to “allow” or “restrict” network accessible services and should the term be adjusted as such?

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We agree with the proposal; however, please update the measures to match. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP offers the following comment for the SDT consideration for Question 6: Recommend the SDT change the word “ports” to the word “services” in the measure, as the requirement was changed to focus on the standards.	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
Referring to the Change Rationale for CIP-007 Part 1.1, DTE recognizes the clear direction shift from "ports" to "services". However, R1.1 infers that a port listing may still be required to justify the service. The “Measures” does not reference “services”. DTE would recommend additional measures that demonstrate potential compliance strategies that do not require the demonstration of “ports”. Without such reference it may be inferred that such a “port” list is a prescriptive requirement, which would not provide any relief to the entity's burden of compliance.	
Likes 0	

Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerns on the definitions caused this no vote for this standard.

The change the requirement title to "System Hardening" is unclear. "System hardening" is used in section 3.1 as an alternative to AV and as part of the TCA/RM requirements.

The TR states, "harden the applicable systems through limiting access to logical services and physical ports" but the requirement language states "Services and logical ports."

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer	No
Document Name	

Comment

FMPA supports Marty Hostler and Northern California Power Agency comments.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

Services are typically associated with Cyber Assets running an operating system. There is no technical or risk basis for changing from ports to services. While an open port is associated with a running process (service), on firmware based Cyber Assets and some software appliances, they do not have the ability to discern the running process (service) which the port is open. Further, part of the attack surface of a Cyber Asset is determined by its open ports. Processes may or may not be discernable. Network accessible ports are consistent across any platform running a TCP stack and can be determined easily. While the new language in the requirement allows for documenting ports as a secondary mechanism, there is not technical merit or risk reduction in documenting services over network accessible ports. This also was not a part of the FERC order or SAR.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	No
Document Name	

Comment

A requirement to control logical ports makes far more sense than services. If services is the term used, services needs to become a defined term. There are many ways to interpret the term services. Windows and Linux each have different approaches to managing and using the term services. Application frameworks use the term differently as well.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

The revision to CIP-007 Requirement Part 1.1 needs to be clarified. The “or” statement will cause different interpretations across regions and auditors.

The proposed use of “system hardening” in CIP-007 is inconsistent and not defined

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

Unnecessary confusion. Previous standard language was sufficient for design of security controls and application. Revert to old standard, which industry has worked hard to standardize and create controls that have been effective.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

R1.2 - Additional clarification is needed to clearly determine what the term “non-programable communications components” means.

R2.1 – As written, it appears that patching can be performed at the “system” level vs at the individual CA level. Additional language should be added to clarify the intent of the team as the current language is ambiguous.

R4.1 – As written, it appears that logging should now be performed only at the system level and does not allow for additional logging at the CA level. Additional language should be added to clarify the intent of the team as the current language is ambiguous.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AEPCO is signing on to ACES comments, please see below:

Services are typically associated with Cyber Assets running an operating system. There is no technical or risk basis for changing from ports to services. While an open port is associated with a running process (service), on firmware based Cyber Assets and some software appliances, they do not have the ability to discern the running process (service) which the port is open. Further, part of the attack surface of a Cyber Asset is determined by its open ports. Processes may or may not be discernable. Network accessible ports are consistent across any platform running a TCP stack and can be determined easily. While the new language in the requirement allows for documenting ports as a secondary mechanism, there is not technical merit or risk reduction in documenting services over network accessible ports. This also was not a part of the FERC order or SAR.

Likes 0	

Dislikes 0

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

Likes 0

Dislikes 0

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE does not agree with the proposed changes to the Measures section of CIP-007 Requirement R1 Part 1.1. The STD should update the Measures to include the “listing of services” instead of keeping the existing “ports” language since it is not consistent with the changes to the Requirement language.

Likes 0

Dislikes 0

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

See MEC and BHE comments.

Likes 0

Dislikes 0

Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree with the proposed changes to the Measures section of CIP-007 Requirement R1 Part 1.1. The STD should update the Measures to include the “listing of services” instead of keeping the existing “ports” language since it is not consistent with the changes to the Requirement language.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
More clarity is needed for the change to this requirement. Are there examples as to where there would be a network accessible service without an associated network accessible port?	
Likes 0	

Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Suggest reviewing the applicable systems column should include SCI hosting High or Medium Impact BCS or their associated: PCA

Suggest reviewing the Requirements column for requirements 1.1 and 1.3, the objective is the same, yet the text isn't. It should have the same level of detail.

Suggest reviewing the Applicable Systems of CIP-007, should include Management Systems.

Suggest not to include PACS and EACMS into the scope in the context of SCI as this requirement doesn't exist for a PACS and EACMS not on a SCI. SAR is intended for virilization concepts, not to add additional controls.

Suggest reviewing the Applicable Systems of CIP-007 associated to management modules. The current langage only refers to a Management Modules of SCI hosting . What about a the management module of a BCA ? Management Modules of SCI hosting would have more controls than a Management Modules of BCA.

Request clarification on the term “system" (cyber security patches for systems). Is the objective for the system to be patched or for the cyber asset composing the system to be patched ?

Request clarification on the term system capability (Log security events, per system capability), logging from one cyber asset would be enough to comply with the requirement ?

Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	No
Document Name	
Comment	

Entergy cannot support this standard as written due to a lack of clarity regarding required documentation and adequate information to inform expected auditing approach. The standard states “or logical network accessible ports if unable to determine service” but the Requirements and the Measures, as well as the lack of a Guidelines & Technical Basis section, do not provide adequate guidance on what documentation is expected to enable only logical network accessible ports as opposed to services. If an entity identifies that they are "unable to determine service", what evidence, if any, would be required by the entity to justify the inability to determine service?

Additionally, although the Requirement has been changed to shift the focus from ports to services, the measures as written still focus on the documentation of ports and makes no mention of services, which leads to ambiguity for the entities on how to achieve compliance.

The SDT is recommended to provide additional clarity regarding evidenciary examples for a.) when the entity is unable to determine service and is instead limiting ports; and b.) update the measures to provide clarity on examples of evidence related to services and/or ports.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We agree with the proposal; however, please update the measures to match.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Part 1.1: Changes focus from ports to services, requiring enabling only needed services. Entity may fall back on port identification only when services cannot be identified. The shift to focusing on looking at services could restrict auditor visibility in the case where a service arbitrarily uses overly large port ranges. The part does include the language “including port ranges where needed to handle dynamic ports” however this would result in the auditor not knowing the port ranges associated with all services deemed necessary. The onus would then be put on the auditor to determine the ports associated with a particular service and whether the port ranges are reasonable or not. In addition, entities focus would be on authorized services and not on the actual system vulnerability of an increased attack surfaced created by ports that are not intentionally disabled. A recommended change may be “Disable all logical network accessible ports except those associated with network accessible services that have been determined to be needed by the Responsible Entity (or logical network accessible ports if unable to determine service, including port ranges where needed to handle dynamic ports), per system capability. If a system has no provision for disabling or restricting network accessible services (or logical ports) then those services (or logical ports), that are open are deemed needed.”	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	

ISO-NE finds the following requirement language unclear, “…network accessible services (or logical ports), that are open are deemed needed.” The language seems subjective and may be interpreted to mean ‘can be open’ or ‘open for a period of time’ which presents a compliance risk. For this reason, ISO-NE recommends defining network accessible services.

Additionally, CIP-007 Part 1.3 conflicts with Part 1.1, both parts should be combined because virtual hosts and physical hosts would run on the same ports. The physical attribute is the only aspect addressing ports; the distinction between virtual vs. physical adds confusion.

ISO-NE appreciates the removal of TFEs and understands that system capability requirements are still in place and will need to be documented.

Likes 0	
Dislikes 0	

Response

Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6

Answer	No
Document Name	

Comment

We agree that a focus on services is warranted, however entities will need clarification of the term “services” to correctly scope their CIP programs.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Comments: We recommend revising SDT’s proposed language.

Recommendation:

- Revise the current CIP-007-6 language to read:

“Enable only logical network accessible ports or services determined to be needed by the Responsible Entity per system capability. If an applicable Cyber Asset or BCS has no provision for disabling or restricting network accessible ports or services on the Cyber Asset or BCS, then those open ports or services are deemed needed.”

Likes 0	

Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
Please consider the following proposed requirement, “The Responsible Entity shall determine which network accessible services are needed and enable only those services (or logical network accessible ports if the Responsible Entity is unable to determine the service, including ports ranges where needed to handle dynamic ports), per system capability. If a system has no provision for disabling or restricting network accessible services (or logical ports) then those services (or logical ports) that are open are deemed needed.”	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Comments: We recommend revising SDT’s proposed language. **Recommendation:** • Revise the current CIP-007-6 language to read: “Enable only logical network accessible ports or services determined to be needed by the Responsible Entity per system capability. If an applicable Cyber Asset or BCS has no provision for disabling or restricting network accessible ports or services on the Cyber Asset or BCS, then those open ports or services are deemed needed.”	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

1. SRP request clarification with the concept “If a system has no provision for disabling or restricting network accessible services (or logical ports) then those services (or logical ports), that are open are deemed needed.”

2. Is this requirement addressing just vitural environements or can the physical environment (current) version also be part of this new requirement. SRP has questions concerning backward compartible if we are not in a virtual environment. Or is this requirement speaking only to virtualization, and if this is the case - physical would have to be backward compatibility.

3. What is the value of removing ports if the phrase “(or logical ports)” is added every time services is used?

Likes 0

Dislikes 0

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Revise to clarify that only "listening ports" are the subject of the requirement. The proposed language does not differentiate between established and listening ports.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0

Dislikes 0

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	
Comment	
EEI supports the proposed shift from logical network accessible ports to services.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 6.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the approach for CIP-007, R1, Part 1.1.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes

Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE agrees with the proposed changes to CIP-007. Texas RE recommends, however, clarity be provided on the term “network accessible services”. While the measure mentions listening ports, there is no language in the requirement clarifying network accessible services.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
LCRA supports this change.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the proposed shift from logical network accessible ports to services.	

Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
LCRA supports this change.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS would like for a clearer definition of what a “service” entails.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
The change does not seem to pose any concerns from ports to services. There still continues to be a disconnect from CIP-007 R1.1 and CIP-010 R1.1. Is there a fundamental reason why CIP-007 R1.1 applies to Medium Impact systems that have ERC but the baselines requirements of CIP-010 R1.1 apply to all Medium Impact systems? Those two sub-requirements seem like they should sync up one way or the other.	
Likes 0	

Dislikes 0

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	Yes
Document Name	

Comment

While CHPD does not disagree with this change, it seems to be unnecessary as CIP-007 R1.1 already requires the entity to demonstrate the need for the port. In doing so, the entity indirectly documents the service by explaining the need for the port.

Likes 0

Dislikes 0

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change

Likes 0

Dislikes 0

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC provides the following comments for the SDT’s review and consideration:

9. In the applicable systems column, the reference to SCI includes an “or” and not an “and.” This creates uncertainty as to whether both “their associated EACMS or PACS” must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are “and” focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

10. In the defined terms, Management Modules are specifically excluded from SCI; however, the applicable systems column references Management Modules of SCI. This verbiage creates the potential for confusion and ambiguity relative to Management Modules. The following clarification is suggest to reduce the potential for ambiguity:

Management Modules supporting [or associated with] SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

No comments

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	Yes
Document Name	

Comment

We agree with the proposal; however, please update the measures to match.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Yes, Southern supports these proposed revisions to shift the security objective to enabled services. Southern also requests that the SDT remove the phrase “per system capability” (along with “Where technically feasible”). The second sentence of R1.1 states that where a system has no provision for … which covers an entity in all situations and therefore a TFE or a “per system capability” exemption is not needed.

Additionally, Southern requests the SDT consider the potential for “double jeopardy” with regulators with regard to CIP-007 R1 and CIP-010 R1 when providing evidence to support compliance for enabled services. Any failure to authorize and document changes to services as per CIP-010 R1 can also result in a potential violation of CIP-007 R1 as services may be enabled without documented authorization; Southern requests the SDT consider modifications to eliminate the duplicative nature of the two requirements and remove the potential for double jeopardy.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

THE SELECTION SHOULD BE NO TO THE QUESTION.. THE SBS SYSTEM WILL NOT ALLOW FOR EDITS AFTER A SELECTION HAS BEEN SAVED.

Duke Energy agrees with the intent of a services based approach but does not agree with the revision as worded. Duke seeks clarification that entities may credit existing port controls and associated evidence without need to re-document explicit approval of services if the ports associated with their use are already approved. In addition, Duke seeks updated measures to provide examples of how services may be documented.

Duke Energy requests the inclusion of the “(or logical ports)” flexibility in Part 1.3 to mirror Part 1.1 particularly since Management Modules are included and are known to have poor documentation on older models such that open port data may only be available from port scans.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	

Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

7. CIP-010 Requirement R1 currently requires Responsible Entities to develop a baseline configuration, authorize changes to the baseline, and document the changes. The SDT proposes to revise Requirement R1 to remove the reference to baseline configurations. The proposed revisions require the authorization of changes to Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible ports, security patches applied, and SCI configurations. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Consider revising to clarify the lower threshold of what is included in the term *baseline.* Otherwise, this language may be interpreted to include administrative changes in nature and have no impact to the cybersecurity posture of the cyber asset.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

1. SRP interpret this to mean providing baselines will not be required for evidence. This does not state anything about physical, only virtual. Please clarify requirements for Physical, and backward compatability.

2. SRP recommends changing logical network accessible ports to logical network accessible services to be in alignment with the other proposed changes. SRP also believes SCI configurations is redundant. SCI configuration is included as part of the “Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible services and security patches applied of the virtualization and storage system.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: Refer to our comments in the QUESTION 1 definitions. Considerations could be existing revised language to meet the intent of the SAR and a revision to CIP-010 R1.1.

A. The baseline documentation requirement represents the current configuration of a BCS/BCA with the objective of maintaining the security posture of the BCS/BCA, otherwise the changes have no basis.

The virtual image shouldn't be captured as a baseline because: 1) for an active virtual image, it should be a VCA that has its own baseline; 2) for a dormant virtual image, it is similar to a powered off physical cyber asset, as long as you maintain a base image for compliance all the time, it can be used when the dormant virtual image is turned on. In addition, the configuration baselines are not for the proposed definitions and applicability for SCI, SCA and management modules (See our comments for Question 1).

Recommendation: Restore CIP-010-3 language.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

Comments: Refer to our comments in the QUESTION 1 definitions. Considerations could be existing revised language to meet the intent of the SAR and a revision to CIP-010 R1.1.

The baseline documentation requirement represents the current configuration of a BCS/BCA with the objective of maintaining the security posture of the BCS/BCA, otherwise the changes have no basis.

The virtual image shouldn't be captured as a baseline because: 1) for an active virtual image, it should be a VCA that has its own baseline; 2) for a dormant virtual image, it is similar to a powered off physical cyber asset, as long as you maintain a base image for compliance all the time, it can be used when the dormant virtual image is turned on. In addition, the configuration baselines are not for the proposed definitions and applicability for SCI, SCA and management modules (See our comments for Question 1).

Recommendation: Restore CIP-010-3 language.

Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No

Document Name

Comment

ISO-NE agrees with the proposed revisions that remove references to baseline configuration because they provide significant relief from baseline tracking and seem to better align with general change management practices. However, the deletion of the term “configuration” from “configuration change management” throughout the revisions may cause a great deal of confusion. Change management covers a wide breadth of “changes” from items considered “baseline configurations” to other non-material changes that do not affect a baseline. Differences in interpretation or definition of “change management” could lead to a dispute with Regional Entities and present a compliance risk. ISO-NE recommends that the SDT make further revisions to clarify which “changes” that require change authorization and testing.

ISO-NE also recommends that the SDT remove CIP-010 R1 Part 1.1.6 and create a new requirement to align the applicability for SCI.

Furthermore, ISO-NE recommends that the added language to CIP-010 R1.3, “...that minimizes difference with the production environment…” be deleted because CIP-010 Part 1.3.2 requires that the differences between the test environment and production environment be documented.

Likes 0

Dislikes 0

Response

Marty Hostler - Northern California Power Agency - 5

Answer No

Document Name

Comment

See Response to Question 1.

Likes 0

Dislikes 0

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer No

Document Name

Comment

In *CIP-003-3 we had requirement R6 that stated “Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.” CIP-010 R1 was developed to put an emphasis* *on configuration management . It now appears CIP-010-5 is reverting back to authorizing a change and not assuring that you have a trusted configuration.*

Baseline management is critical for system integrity, being able to detect and correct unauthorized changes, and insure that machines are properly configured, patched, and up-to-date. Removing the requirement to maintain baseline configurations will leave significant security gaps, would lead to significant visibility issues into the configuration state of the Cyber Asset, ultimately leaving Responsible Entities blind to unknown vulnerabilities within the Cyber Assets. Baselining tools are becoming more and more capable of automating the process for baselining an Entities' environment – so there is no reason to strip this out of the standard. Even with the addition of virtualization, one would be able to baseline (and monitor baselines) for any virtual machines that the entity uses.

R1.4 will require entities to monitor for unauthorized changes. Unless they have a baseline to compare to, they will not be able to know when a change is made.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We agree with this approach. This reduces administrative burden.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

Likes 0	
Dislikes 0	

Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	No
Document Name	
Comment	
CHPD agrees with the changes, but as stated before, CHPD does not agree with the CPU and memory isolation requirements. The affinity rules should not be included in the list of configuration items that require authorization for change.	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	No
Document Name	
Comment	
While Entergy does agree with the approach being suggested, the switch from a port focus to a services focus adds an additional challenge. Network services are generally difficult to identify programmatically since many can be configured off default registered ports or use ports in theephemeral ranges that change with each use. The wording used here would seem to indicate that ports can only be used if the service cannot be identified, this would certainly lead to requiring a mixture of methodologies used for identification for each device. Entergy would recommend this wording be changed to identify that either the port or the service should be identified to give entities the flexibility to use either in order to maintain consistency in their program, which would reduce human performance errors. Additionally, more definition should be wrapped around what the Regulator means by service? Do they mean the network protocol or the service running on the asset that is network accessible. An example would be do they want https or Apache Web Service identified? This lack of definition would make it difficult to identify what monitoring would need to be put in place and what evidence would need to be gathered to meet this standard.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	No

Document Name	
Comment	
It is not clear if the maintenance and upkeep of the current baseline and previous baselines is still required. BC Hydro SME team requests that the wording of the CIP-010 Requirement R1 be clarified to reflect if baselines are not needed any more. The technical rationale for CIP-010 R1 also needs more clarity if the previous baselines are required to be maintained as change records (time period until they should be kept as record and maintained) and what additional controls are proposed, if any, if the baseline is only one of the controls.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Please provide additional clarification and contextually relevant guidance to draw out the SDT's intent with the definition of "SCI." Moreover, the inclusion of baseline elements requires more context to the new term "SCI."	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No

Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AEPCO is signing on to ACES comments, please see below: The question does not include the new definition for Self-Contained Application, so ACES cannot answer "Yes." . ACES suggests removing the definition and term "Self-Contained Application" .	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
It is unclear if the addition of "The production environment does not include devices being actively remediated and logically isolated." indicates that assets currently listed in a remediation action plan do not need to be included in annual CVA.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No

Document Name	
Comment	
SDT has created an uncalled for scenario where they have removed Baselines but left the baseline elements intact, which is causing significant confusion amongst SMEs. Requiring CM as method of compliance will set a serious challenge and will limit ability to secure system as CMs do not include security baseline information, only the proposed changes, but assessments are never included in CM, just a summary of results. This whole approach will result in inaccurate and subjective application and often result in contention with compliance and auditors. Current CIP-010 standards and requirements are matured and industry has made significant progress developing good controls. There is absolutely no reason to change as these changes do not improve security but are detrimental.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
CIP-010 R1, request that the SCI requirement into a separate Part. Remove the “OR” statements in Part 1.1. Applicable Systems. Placing the SCI requirement into a separate Part could resolve this	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE is concerned security obligations will be reduced by removing the reference to baseline configurations. Establishing and maintaining baseline configurations represent best practices for system hardening. Texas RE recommends adhering to NIST Special Publication 800-53 (Rev. 4), CM-2 Baseline Configuration, which states, “*Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture*.”	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
The question does not include the new definition for Self-Contained Application, so ACES cannot answer "Yes". ACES suggests removing the definition and term "Self-Contained Application".	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	
FMPA supports Marty Hostler and Northern California Power Agency comments.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard. We agree with the removal of the administrative function of documenting a baseline.	

Request c “minimal differences” be changed to “minimal differences, as determined by the entity”

Many of the Applicable Systems use only AND – some Applicable Systems use “OR” . For example, Part 1.1 says “SCI hosting High or Medium Impact BCS or their associated:” It is the "or their associated” that is in question. This probably means that the SCI is applicable but this is not clear.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

SPP offers the following comments and questions for the SDT consideration for Question 7:

Recommend the SDT provide an interpretation of the definition for Self-Contained Application. As written, the definition seems confusing, and could have the potential to be misinterpreted.

Is the SDT asking for entities to include both firmware and OS? In the past, entities could not show firmware if an OS was present. This has the potential to broaden the scope, and includes authorized changes to the OS. Any changes to the OS would be included in scope and would have to be tested as part of 1.4 and 1.5. In the past, if the baseline was not changed, then the entity would not have concern about R1.4 and 1.5. This new standard will change that, and potentially add additional work for entities when a change is made. This could open entities to an investment in new tools because baseline is being removed.

Recommend the SDT define and provide an interpretation in the scope of what it means by “Authorized Changes”.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

We agree with this approach. This reduces administrative burden.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

Likes 0	

Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the SRC.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Three comments on R1.3. These comments are repeated for CIP-010 R3.2. 1) request removal of “minimizes differences with the production environment” because new language is a) subjective, b) better suited to the measures and c) the previous language is sufficient 2) if this language cannot be removed, request clarification that the entity determines “minimal differences” 3) suggest that the intent is to a) test and b) document what was tested. CIP-010 R1, request that the SCI requirement into a separate Part. Same comment made for CIP-010 R1. Request clarification – there are several ways to read the nested ORs included in the Applicable Systems section for SCI. Many of the Applicable Systems use only AND – some Applicable Systems use OR. For example, Part 1.1 says “SCI hosting High or Medium Impact BCS or their associated:” Suggest reviewing the definition for better clarity.	
Likes 0	
Dislikes 0	
Response	

Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy recommends changing logical network accessible ports to logical network accessible services to be in alignment with the other proposed changes. SCI configuration is included as part of the “Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible services and security patches applied of the virtualization and storage system.	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes proposed changes beyond those needed for conformance: Have little or nothing to do with virtualization, Are unlikely to improve anyone’s cyber security posture, Are outside the scope of the original 2016 SAR, Are not addressed in any relevant FERC Order, and	

Would be an unnecessary and unwelcome distraction for entities trying to adjust their CIP programs and documentation to accommodate new virtualization-related requirements.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

Please see comments submitted by the ISO/RTO Council Standards Review Committee.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization

Answer	No
Document Name	

Comment

CIP-010, R1 - Removing “baseline configuration” does not change what needs to be done in practice. Entities will still need to retain a baseline configuration as evidence from which to establish the changes that were authorized. The proposed change decreases clarity (in terms of what must be done to demonstrate compliance).

Recommendation: Reinstate the concept of “*baseline configuration.*”

CIP-010, R1 - Likewise, removing the word “configuration” from the term “configuration change management” (both in the title of CIP-010, Table R1 and throughout the text of R1), may cause a great deal of confusion since the more generic term, “change management,” can be interpreted to include a wider breadth of “changes” than those limited to “baseline configuration” and may substantially expand the scope of this requirement with other non-material changes.

Recommendation: Reinstate the term “*configuration change management*” in the title of CIP-010, Table R1 and throughout the text of R1.

Part 1.1.3 – Typically, Self-Contained Applications are considered custom software which is already covered under the existing standard and as such would not require a revision.

Recommendation: Explain why this clarification is needed.

Part 1.1.4 – SRC agrees that logical network accessible ports alone only tell part of the story and supports the SDT's proposal to include services. That said, the shift away from logical network accessible ports to services does not significantly change the security benefit achieved; however, it does make it more difficult for an entity to define and may imply that defined ports do not need to be included.

Recommendation: SRC recommends the SDT retain the concept of ports and define a new term, "ephemeral ports;" i.e. the listening ports that initiate the conversation, as a focal point for protection and security. This would allow the industry to move away from port ranges.

Part 1.1.6 – The first three bullets are very specific and well defined. The fourth bullet is very vague and draws in everything else that is not defined, making it very difficult for entities to comply with.

Recommendation: Clarify the types of services intended by the fourth bullet so there is consistency across the ERO.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO signs on in support of SRC.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the proposed modifications to revise Requirement R1 to remove the reference to baseline configurations.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the SDT's direction here to provide a forward-looking, objective-based requirement and eliminate the documentation exercise of maintaining baseline inventories. However, for R1.1.2, Southern requests the SDT consider adding the concept of "installed" back as it is done in R1.1.3. Also, please consider re-ordering the proposed requirements in order to potentially split requirements for stand-alone systems and Self-Contained Applications. For example, R1.1.3 could focus on authorizing change to the SCAs when they are changed in a repository and not as they are automatically deployed from there to each 'applicable systems'. Additionally, we request the SDT provide further guidance on the components of "SCI configurations" for which changes must be authorized. The bulleted list in CIP-010 R1.1.6 provides some guidance but is not encompassing. Under CIP-010 R1.1.6, Southern requests that the SDT consider removing the first bulleted item "Enforces electronic access controls that…" as that is essentially the same as the second bulleted item "Enforces logical isolation between…"	

Under CIP-010 R1, Southern requests the SDT consider addressing the scenario, and provide alternative requirement language, as to “when” authorization has to occur. For example – are changes to a virtual desktop image residing in a BCSI repository required to be authorized at the time the image is updated, or when the updated image is deployed into a production environment? Or both?

Under CIP-010 R1.2, Southern requests the SDT consider removing Part 1.2.1 based on its lack of practicality. In recent audits of this requirement Part, auditors have expressed the expectation that Part 1.2.2. should include a check of all security controls to ensure they were not adversely impacted, thereby making the performance of Part 1.2.1. moot. Additionally, Southern recognizes that with many types of changes, it is not possible to predict all possible security controls changes that may take place with a change, and therefore most entities have adopted best practices to thoroughly check security controls following the change, making Part 1.2.1 useless from a security standpoint.

Additionally, Southern is concerned that the language in CIP-010 R2.1 would still force entities to maintain “documentation” the same as or similar to a “baseline configuration” in order to comply with R2. Southern requests the SDT consider this dilema and possibly propose alternative language for R2 that would align it with the proposed changes to R1. For example – in R2, the phrase “items described in R1, Part 1.1” are essentially the components of the former “baseline”; in order to monitor those items every 35 days for changes to those items, you must first have documentation, lists, or scan results of those items so that you can compare and detect any unauthorized changes to them. Likewise, the requirement does not dictate that an entity must monitor authorized changes, but only “unauthorized” changes. Therefore, for an entity at audit that has had no “unauthorized” changes, the activity can become a deep-dive “prove-the-negative”.

To align the direction of R1 towards “change management”, Southern requests the SDT consider removing the word “configuration” in the Measures of R2.1 and replace it with something akin to:

R2.1: An example of evidence may include, but is not limited to, documentation or logs showing that monitoring for changes to the items in Part 1.1 is conducted, along with records of investigation for any unauthorized changes that were detected.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	Yes
Document Name	

Comment

We agree with this approach. This reduces administrative burden.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

No comments	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes that the verbiage should be updated to reflect logical network accessible **services** as opposed to ports.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change and agrees with comments provided by EEI for this survey question	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	

There is no timeline for authorizing changes, but we like the option to define that timeline ourselves. There should be a provision for urgent changes – like zero day vulnerabilities, that would allow authorization after a change has occurred.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC provides the following comments for the SDT’s review and consideration:

1. Consider whether the purpose statement should be revised to address the broader scope of the proposed revisions.

2. In the applicable systems column, the reference to SCI includes an “or” and not an “and.” This creates uncertainty as to whether both “their associated EACMS or PACS” must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are “and” focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

3. In the defined terms, Management Modules are specifically excluded from SCI; however, the applicable systems column references Management Modules of SCI. This verbiage creates the potential for confusion and ambiguity relative to Management Modules. The following clarification is suggest to reduce the potential for ambiguity:

Management Modules supporting [or associated with] SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS

4. In requirement R1.1.6, the following revision is recommended for clarity:

1.1.6. Enforces electronic access control that permits only controlled communications that are [needed/necessary] between systems with different impact ratings hosted on SCI.

5. In the proposed revisions for requirement R1.3.1, the proposed verbiage is unclear. The following revision is recommended for clarity:

1.3.1. Prior to implementing any authorized change in the production environment, except during a CIP Exceptional Circumstance, test the authorized changes in a test environment that has minimal, documented/authorized differences when compared with the production environment…

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change and agrees with comments provided by EEI for this survey question	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Suggest reviewing the definition for better clarity.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	

Answer	Yes
Document Name	
Comment	
This change seems somewhat negligible. Auditors will still likely expect similar documentation as they always have to ensure that all changes are captured and approved and that there is a complete population to audit. The theory and objective of the changes seem sound but the actual benefit of these changes seem as if they will be minimal.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes

Document Name	
Comment	
AEP supports changes regarding baseline configurations. While baselines will remain a critical record for entities to maintain, they should not be used for compliance purposes. Instead, we agree with the modifications that place the emphasis on monitoring unauthorized changes (to the items described in Requirement R1, Part 1.1). The process of tracking and maintaining records for all changes to a baseline represent an unnecessary compliance burden that offers few protections yet places burdensome recordkeeping on entities for no material reliability benefit.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
There is no timeframe clarified in CIP-010 R1 for the authorization to occur. Suggest clarifying as: “Prior to the change, authorize changes to:” as the lead in statement. We further suggest that if this change is made that the CEC Exception also be included to allow for emergency change to be performed ahead of formal documented authorization.	
Likes 0	
Dislikes 0	
Response	

David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change and agrees with comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes

Document Name

Comment

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-010, R1,   PG&E supports the modfications and the input provided by EEI.

Likes 0

Dislikes 0

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb

Answer Yes

Document Name

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 7.

Likes 0

Dislikes 0

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer Yes

Document Name

Comment

EEI supports the changes regarding baseline configurations. While baselines will remain a critical record for entities to maintain, they should not be used for compliance purposes. Instead, we agree with the modifications that place the emphasis on monitoring unauthorized changes (to the items described in Requirement R1, Part 1.1). The process of tracking and maintaining records for all changes to a baseline represent an unnecessary compliance burden, that offers few protections yet places burdensome recordkeeping on entities for no material reliability benefit.

Likes 0

Dislikes 0

Response

Trevor Tidwell - Trevor Tidwell - 1,3

Answer	Yes
Document Name	
Comment	

While we appreciate the revisons to CIP-010 R1, is the expectation that we would just need to provide a set of tickets where we said the baseline changed, but not have to back it up with baseline documentation? Would the change ticket now need to be in more detail to clearly indicate what element(s) of CIP-010 R1.1 changed so we don't have to provide baseline documentation? For example, “updated Windows machines with patches for released in {MONTH] {YEAR}” or “updated machine X with SFTP service”? PNMR expresses support of comments by John Galloway, On Behalf of: Michael Puscas, ISO New England, Inc.

Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	
Document Name	

Comment

Please see comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

8. The SDT modified CIP-010 Requirement R3 Part 3.3 to ensure that vulnerability assessments are performed prior to logically connecting Cyber Assets, VCA, and SCI. The revised requirement allows the use of remediation VLANs to perform active vulnerability assessments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	

CAISO signs on in support of SRC.

Likes 0	
Dislikes 0	
Response	

Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	No
Document Name	
Comment	

The SRC greatly appreciates the following changes and clarifications proposed by the SDT:

- Part 3.2: addition of “*per system capability*”
- Part 3.3: use of “*previously assessed configurations*” allows for the use of gold images

Recommendations:

- Replace the last sentence of Part 3.3; i.e. "*The production environment does not include devices being actively remediated and logically isolated*," with the following: "*Remediation or mitigation action items must be completed prior to production use*." This meshes with Part 3.4 and clarifies that all vulnerabilities must be remediated prior to production use as opposed to remediated prior to placing in an ESP environment.
- Clarify that annual active vulnerability assessments would not require the use of remediation VLANS

Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	No
Document Name	
Comment	
Request explanation. This language is about "connecting." Elsewhere language is about "isolating." Please explain this switch. Request clarification - what is the change when discussing physical connection or active communication? Request clarification of the requirement because the OR is confusing. Would it be easier to understand with two sentences instead of one long sentence? Request clarification of the first and last sentences in this requirement. What is the difference between "logically isolated" and "not logically connected?" Please clarify how to read the first sentence's ORs.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The use of an undefined term, “logically connecting” has the potential to create confusion when included within a NERC CIP Reliability Standard Requirement. The Standard Processes Manual provides direction for when a NERC Glossary of Terms definition is needed, notably that certain criteria should determine whether a new or revised definition is needed (see Appendix 3A (ROP) Standard Processes Manual, Section 5.1). The primary factor for determining whether a NERC defined term is needed rests on whether the term can be understood using a standard collegiate dictionary. For many IT terms commonly in use, the standard collegiate dictionary is rarely helpful. For example, the term logically connected is not defined by Merriam-Webster. The NIST Information Technology Laboratory (Computer Security Resource Center On-line Glossary of Terms (https://csrc.nist.gov/glossary) includes “logically connecting” and similar terms such as “logically connected, logical connection, etc.” Unfortunately, a definition that aligns with the term “logically connecting” that might provide insights necessary to ensure that those responsible for compliance have a common understanding of what is being proposed in Requirement R3, Part 3.3. is unavailable. EEI recommends the term be defined or direction be provided within the Technical Rationale to ensure a consistent understanding. EEI requests for clarification whether cyber vulnerability assessments must be performed in the VLAN environment and then switched to production.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb	
Answer	No
Document Name	
Comment	

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 8

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request explanation. This language is about “connecting.” Elsewhere language is about “isolating.” Please explain this switch.

Request clarification - what is the change when discussing physical connection or active communication?

Request clarification of the requirement because the OR is confusing. Would it be easier to understand with two sentences instead of one long sentence?

Request clarification of the first and last sentences in this requirement. What is the difference between “logically isolated” and “not logically connected?” Please clarify how to read the first sentence’s ORs.

Suggest reviewing the definition for better clarity.

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the SRC.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We support the concept; however, we need more information on the use of remediation VLANs and the evidence required. Please consider a webinar and/or additional details in the technical rationale. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-010, R3, Part 3.3. PG&E does have concerns and supports the input provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP Votes **YES** to this one with no comments. This is an edited response and the button option to change the vote is grayed out. Thank you.	
Likes 0	
Dislikes 0	
Response	

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	
FMPA supports Marty Hostler and Northern California Power Agency comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Request explanation. This language is about “connecting.” Elsewhere language is about “isolating.” Please explain this switch.

Request clarification - what is the change when discussing physical connection or active communication?

Request clarification of the requirement because the OR is confusing. Would it be easier to understand with two sentences instead of one long sentence?

Request clarification of the first and last sentences in this requirement. What is the difference between “logically isolated” and “not logically connected?” Please clarify how to read the first sentence’s ORs.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

Too much compartmentalization based on non-industry standard definition. Please review NIST Publication 800-125 (virtualization guidelines) and apply controls, based on Terms such as Management Systems, Guest, Hosts, Network virtualization, Infrastructure virtualization (Mixed Trust, Resources sharing, high-watermarking) and similar guidance that is used by Industry, SME and vendors. SDT approach is complicated and confusing which will result in different interpretation by SMEs and ERO.

Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
The use of an undefined term, “logically connecting”, has the potential to create confusion when included within a NERC CIP Reliability Standard Requirement. Additional clarification is needed on whether cyber vulnerability assessments are required to be performed in the VLAN environment and then switched to production, or could a VCA or SCI be built in its production environment but not activated until the cyber vulnerability assessment is performed and is determined to be ready for activation in the production environment.	
Likes 0	

Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS agrees with the need for a definition of “logically connecting”. This would allow the removal of human error traps associated with a vague interpretation of the definition down the road.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not agree with the proposed changes since it is not clear how an entity is to perform a true vulnerability assessment on a Cyber Asset unless it is connected to the target network. Connecting a Cyber Asset to a network other than the target network will net differing results and require the reconfiguration of the Cyber Asset from the remediation network to the target network.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	

Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree with the proposed changes since it is not clear how an entity is to perform a true vulnerability assessment on a Cyber Asset unless it is connected to the target network. Connecting a Cyber Asset to a network other than the target network will net differing results and require the reconfiguration of the Cyber Asset from the remediation network to the target network.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
As stated earlier, logical isolation is not a defined term. We would like to see an actual definition for "logical isolation"	
Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

Oklahoma Gas and Electric supports the comments provided by EEI.

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

R3.3 ‘The production environment does not include devices being actively remediated and logically isolated.’ The language of this requirement lacks clarity around undefined terms: ‘logically connecting’, ’additional’, ‘devices’, ‘remediated’, and ‘logically isolated’, resulting in unenforceability. The requirement does not include consideration of CPU/memory sharing as seen with other logically isolated systems. The language also seems to be somewhat circular in that the ‘production environment’ includes an exclusion after the requirement language.
Suggested Comment:

R2.1 lacks inclusion of SCI and Management Systems for High Impact BCS and associated EACMS, PCAs. This does not align with their inclusion in most of the other requirements within the standard and reduces the protections required under the current standard language. The technical rationale does not address why it is not needed for SCI.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We support the concept; however, we need more information on the use of remediation VLANs and the evidence required. Please consider a webinar and/or additional details in the technical rationale.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

Likes 0	
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

It is unclear to us whether a scan will be needed for all installations and that the previous concept of a group of baselines is no longer acceptable. This amount of additional work is excessive and does not alleviate any additional cybersecurity risk. We request that the SDT make it very clear using a scan from a previously installed Cyber Asset, VCA or SCI that is similarly configured is acceptable to demonstrate compliance with R3.3.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Remediation VLANs are not defined and may introduce situations where an entity could inadvertently place production Cyber Assets in this VLAN.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	

Comment
CIP-010 Requirement R3 Part 3.3 uses the undefined term "previously assessed configuration" which could be interpreted as a byte-for-byte copy of a golden image, or could be referring to the items defined in Part 1.1. ISO-NE has concerns that the industry will gravitate to the most conservative interpretation of the term. ISO-NE recommends that the SDT include Part 1.1 items in Part 3.3 to further clarify this requirement. ISO-NE recommends that the SDT clarify the level of logical isolation that is expected to keep the device out of the production environment when using a remediation VLAN.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	No
Document Name	

Comment
Logically connected should be further defined to reduce the likelihood of misinterpretation.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	

Comment

Comments: The revisions to CIP-010-3 R3.3 are not clear (See our comments for QUESTION 1). We have not observed challenges with remediation VLANs in the existing CIP requirements. This is because remediation VLANs can be managed within the ESP as a hot standby VLAN when connected to a layer 2 (data link) BCA switch or connected to a non-CIP switch.

The language “The production environment does not include devices being actively remediated and logically isolated” does not resolve security concerns; i.e., depending on what type of logical isolation is acceptable? Additionally, this term is subjective. If logical isolation is allowable for a non-ESP model, it could also be allowable for an ESP model meaning as long as a Remediation VLAN is logically isolated from the BCS VLAN on the same switch, it doesn’t need to be within the ESP.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: The revisions to CIP-010-3 R3.3 are not clear (See our comments for QUESTION 1). We have not observed challenges with remediation VLANs in the existing CIP requirements. This is because remediation VLANs can be managed within the ESP as a hot standby VLAN when connected to a layer 2 (data link) BCA switch or connected to a non-CIP switch.

The language “The production environment does not include devices being actively remediated and logically isolated” does not resolve security concerns; i.e., depending on what type of logical isolation is acceptable? Additionally, this term is subjective. If logical isolation is allowable for a non-ESP model, it could also be allowable for an ESP model meaning as long as a Remediation VLAN is logically isolated from the BCS VLAN on the same switch, it doesn’t need to be within the ESP.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

These changes allow for more flexibility regarding VAs in virtual space. However, consider revising language to be more outcome-based, e.g., reducing the risk to BCS's inherent introduction of new cyber assets and/or technologies.

Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE seeks clarification as to whether the SDT is using the phrase “logically isolated” in the same context as proposed CIP-005-7.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
In CIP-010 R3 Part 3.3, the use of “device” doesn’t appropriately cover virtual machines or Virtual Cyber Assets. Therefore, Tacoma Power recommends the following change: “The production environment does not include systems or components being actively remediated and logically isolated.”	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Suggest reviewing the definition for better clarity.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
CHPD supports the efforts of the SDT here to make deployment and remediation of devices easier.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes

Document Name	

Comment

GSOC provides the following comments for the SDT’s review and consideration:

1. Generally, the formatting of applicable systems within the applicable systems column should be evaluated for consistency of format.

2. In the applicable systems column, the reference to SCI includes an “or” and not an “and.” This creates uncertainty as to whether both “their associated EACMS or PACS” must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are “and” focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

3. In the defined terms, Management Modules are specifically excluded from SCI; however, the applicable systems column references Management Modules of SCI. This verbiage creates the potential for confusion and ambiguity relative to Management Modules. The following clarification is suggest to reduce the potential for ambiguity:

Management Modules supporting [or associated with] SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS

4. In the proposed revisions for requirement R3.2.1, the proposed verbiage is unclear. The following revision is recommended for clarity:

3.2.1. Perform an active vulnerability assessment in a test environment that has minimal, documented/authorized differences when compared with the production environment…

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	

Comment

Would like to see the standard require a credentialed vulnerability assessment vs an active vulnerability assessment per asset capability and/or allow for passive analysis which is less intrusive and often more effective than active scans.

Likes 0	
Dislikes 0	

Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
We support the concept; however, we need more information on the use of remediation VLANs and the evidence required. Please consider a webinar and/or additional details in the technical rationale.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the SDTs direction for CIP-010 R3 Part 3.3 to allow remediation VLANs to perform active vulnerability assessments.	
Likes 0	
Dislikes 0	

Response

Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6

Answer	Yes
Document Name	

Comment

We agree with the introduction of remediation VLANs, however, for the sake of backwards compatibility, wording should be added for physical vulnerability assessment tools that would reside on a physical test network for non-virtualized or hybrid environments.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees with the proposed modifications to ensure that vulnerability assessments are performed prior to logically connecting Cyber Assets, VCA, and SCI. Duke Energy recommends adding clarity on what constitutes “logically connecting”.

Duke Energy noticed that the approach and requirement language here seem inconsistent with the language in proposed CIP-005 requirements. It is not clear if it is intent that only the network interface for a VCA must be logically isolated into the remediation VLAN, or if the CPU/memory-sharing isolation requirements apply as well. Conceptually the intent makes sense, but the standard should be clear about what level of logical isolation is expected to keep the device out of the production environment when using a remediation VLAN.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	

Please see comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	

9. CIP-002-5.1a includes exemption 4.2.3.2, which exempted Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. In the development of conforming changes, the SDT determined that the exemption should be split into two distinct exemptions to adequately cover all cyber systems associated with conforming changes. The SDT established those conforming changes in proposed Exemptions 4.2.3.2 & 4.2.3.3. Do the changes clearly identify the exempted cyber systems? If not, please provide the basis for your disagreement and an alternate proposal.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Proposed language lacks the clarity to provide a consistent application.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

1. As SRP reads the definition of what is in scope is not clear from what is stated in the exemption. Clarity is needed due to the vagueness with more details or more of an explanation.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: Due to the use of the ‘logical isolation’ term, and SCI term the changes to 4.2.3.2 & 4.2.3.3 are not needed.

A. Based on our comments in QUESTION 1 and Question 2, the logical isolation for non-routable connections between CIP Cyber Assets is not required by the SAR. The current exemption for communications equipment and links between ESPs implies multiple physical locations.

B. If the SDT intended to address the exclusions of discrete communications links between ESPs, then we suggest a revision to CIP-006-6 R1.10. If NERC is interested in addressing confidentiality and integrity between multiple ESPs (i.e., a super ESP), then we suggest a new SAR to add additional requirements.

Recommend:

- modifying 4.2.3.2 and removing 4.2.3.3.
- Change 4.2.3.2 to clarify the discrete ESPs to span one or more geographic locations such as:

“Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters, and where an individual ESP spans one or more geographic locations.”

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

Exemption 4.2.3.3 needs to be revised to provide further clarity. This appears to be an exclusion for “cyber systems” associated with communication links between discrete ESPs. The new language doesn’t provide the clarity of the approved exemption.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Comments: Due to the use of the ‘logical isolation’ term, and SCI term the changes to 4.2.3.2 & 4.2.3.3 are not needed.

Based on our comments in QUESTION 1 and Question 2, the logical isolation for non-routable connections between CIP Cyber Assets is not required by the SAR. The current exemption for communications equipment and links between ESPs implies multiple physical locations.

If the SDT intended to address the exclusions of discrete communications links between ESPs, then we suggest a revision to CIP-006-6 R1.10. If NERC is interested in addressing confidentiality and integrity between multiple ESPs (i.e., a super ESP), then we suggest a new SAR to add additional requirements.

Recommend:

- modifying 4.2.3.2 and removing 4.2.3.3.
- Change 4.2.3.2 to clarify the discrete ESPs to span one or more geographic locations such as:

“Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters, and where an individual ESP spans one or more geographic locations.”

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

The replacement of Cyber Assets (a defined term) with cyber systems (an undefined term) introduces ambiguity and requires a Registered Entity to self-define cyber systems. This can lead to misinterpretations and disputes between Regional Entities and Registered Entities.

ISO-NE recommends either defining “cyber systems” or reverting back to the defined term Cyber Assets.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
CIP-002-7, 4.2.3.2. states: “Cyber systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).” To ensure that this is properly understood *a definition of “logical isolation” is required.*	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
We appreciate the effort to be consistent with the other exemptions. We do not agree that the exemptions for 4.2.3.1, 4.2.3.2 and 4.2.3.3 clearly identify the exempted cyber systems. We believe term “cyber systems” indicates a broader scope than is intended. This could lead to developing each “cyber system” construct that could lead to under or over scoping BES Cyber System assets for CIP-002. We believe that “systems” as used in the other exemptions relates to things that are categorized beyond “cyber systems”. We do recognize “systems” could include cyber systems at these related assets. Example for 4.2.3.2 & 4.2.3.3: An entity could scope a cyber system as a communication system where the system would reasonably include substation RTUs, channel banks, digital cross connects, microwave radios, etc. Although in our current version, many entities have included RTUs as BES Cyber Assets, the proposed change would lend to 1) removing RTUs from our CIP Programs or 2) expanding the net to Cyber Assets that have been considered part of the current exception because they are now included as part of the communication system. We realize there are ways around this example, but we wanted to highlight this for the purposes of our discussion. For exemption 4.2.3.1 consider removing “cyber” as shown in the following edit: **4.2.3.1.** Systems at Facilities regulated by the Canadian Nuclear Safety Commission.	

For exemptions 4.2.3.2 & 4.2.3.3, we suggest keeping the exception scope to assets that are defined NERC Glossary terms as shown below:

4.2.3.2. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

Also, please provide clarification why the edits included reducing from “communication networks and data communication links” to just “communication links.”

Note: These comments apply to all of the standards in this ballot.

Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Suggest clarification on the geographic locations.	

Request clarification – is the cyber system equivalent to Cyber Asset? We note that Cyber Asset is a defined term. Cyber system is not a defined term.

Request clarification that 4.2.3.2's updates are equivalent to the previous language. Are the demarcation points the same? Explicit exclusions set better expectations

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We appreciate the effort to be consistent with the other exemptions. We do not agree that the exemptions for 4.2.3.1, 4.2.3.2 and 4.2.3.3 clearly identify the exempted cyber systems. We believe term "cyber systems" indicates a broader scope than is intended. This could lead to developing each "cyber system" construct that could lead to under or over scoping BES Cyber System assets for CIP-002. We believe that "systems" as used in the other exemptions relates to things that are categorized beyond "cyber systems". We do recognize "systems" could include cyber systems at these related assets.

Example for 4.2.3.2 & 4.2.3.3: An entity could scope a cyber system as a communication system, where the system would reasonably include substation RTUs, channel banks, digital cross connects, microwave radios, etc. Although in our current version, many entities have included RTUs as BES Cyber Assets, the proposed change would lend to 1) removing RTUs from our CIP Programs or 2) expanding the net to Cyber Assets that have been considered part of the current exception because they are now included as part of the communication system. We realize there are ways around this example, but we wanted to highlight this for the purposes of our discussion.

The exemption language in section 4.2 of every CIP standard will need to be addressed.

For exemption 4.2.3.1 consider removing "cyber" as shown in the following edit:

4.2.3.1. Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

For exemptions 4.2.3.2 & 4.2.3.3, we suggest keeping the exception scope to assets that are defined NERC Glossary terms as shown below:

4.2.3.2. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations. Also, please provide clarification why the edits included reducing from “communication networks and data communication links” to just “communication links’”	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
We support the NPCC TFIST and RSC comments and submit the following additional comments:	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved: Management Module Management Systems Self-Contained Application Shared Cyber Infrastructure	
Likes 0	

Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	10287_1_2016-02_Virtualization_Unofficial_Comment_Form_01222021_MH.docx
Comment	
See attachment for comments.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree with the proposed changes since they do not clearly identify the exempted cyber systems. The new version uses the undefined term cyber systems as opposed to the original using the defined Cyber Assets term. CEHE agrees that revisions are needed since the original resulted in equipment used by carriers to be exempted while the same equipment used by a Registered Entity on a private communications network was considered in scope. The following changes have been proposed. 4.2.3.2. Cyber assets whose function is only to provide connection to external communication networks, as defined by demarcations set by the Registered Entity, that are logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).	

4.2.3.3. Cyber assets whose function is only to provide connection to external communication networks, as defined by demarcations set by the Registered Entity, between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

See MEC and BHE comments.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE does not agree with the proposed changes since they do not clearly identify the exempted cyber systems. The new version uses the undefined term cyber systems as opposed to the original using the defined Cyber Assets term. SIGE agrees that revisions are needed since the original resulted in equipment used by carriers to be exempted while the same equipment used by a Registered Entity on a private communications network was considered in scope. The following changes have been proposed.

4.2.3.2. Cyber assets whose function is only to provide connection to external communication networks, as defined by demarcations set by the Registered Entity, that are logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber assets whose function is only to provide connection to external communication networks, as defined by demarcations set by the Registered Entity, between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	
Comment	
It is still unclear what the phrase “logical isolation” will mean as it gets implemented in many different scenarios provided in this draft of the standards even though it has been used as an accepted term in the explanations provided with these drafts. Exemption 4.2.3.3. also uses this phrase as if it will be universally clear what devices will be used in the implementation of logical isolation. Logical isolation is not a defined term, and though it is attempting to be used as a replacement for ESP, plus more, there are many changes to the standards that are not places where ESP was used or required, and now logical isolation is being used as a universally accepted term without examples or further discussions. The exemptions as listed do not make it clear where that line of demarcation will be nor have examples been provided in meaningful ways. Similar to when CIP-003 was released, there were many diagrams and explanations provided to help entities walk through the different scenarious that could be used in implementation and to convey the intent of the standard.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS does not believe these changes clearly identify the exempted cyber systems. We believe that the undefined term “logical isolation” causes an unclear interpretation. We also feel that the exclusion of the “communication networks” could expand the scope of what’s needed to remain compliant.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
Changes made to CIP-002 exemptions noted in 4.2.3.2 and 4.2.3.3 do not provide a clear understanding of what is exempted because both use terms that are undefined. For 4.2.3.2, the defined term “Cyber Asset” has been replaced by an undefined term “cyber system”. Additionally, the currently approved CIP-002-5.1a exempts communication networks and communication links between discrete ESPs, while the proposed new CIP-002-7 Reliability Standard only exempts the communication links thus implying that the communication networks may now be subject to CIP Requirements.	

In order to clearly define exempted Cyber Assets associated with communication networks, it is necessary for the Registered Entity to clearly designate the communication network components since communication network, communication systems or communication assets have no NERC definition. The following changes have been proposed;

- 4.2.3.2. Cyber Assets associated with communication networks, as defined by demarcations set by the Registered Entity, logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).
- 4.2.3.3. Cyber Assets associated with communication networks, as defined by demarcations set by the Registered Entity, between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

Lastly, the undefined term “logical isolation” is used in both exemptions. As stated in our comments for Question 1, this term should be defined to ensure a clear and common understanding of both the Requirements and Exemptions are contained within the body of CIP Reliability Standards.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AEPCO is signing on to ACES comments, please see below:

ACES does not agree with the new language. The definition of a Cyber Asset is very clear and well known by the industry. The new language “cyber systems” is not defined and could be interpreted differently by entities and auditors. An Entity can point to specific Cyber Assets easily. We also feel this change was not a part of the FERC order or in the scope of the SAR.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

The language in *4.2.3.3* is problematic. It is unclear assets are performing the logical isolation in the Requirement. Cyber systems or the Cyber Assets, Virtual Cyber Assets, or SCI? While Dominion Energy is of the opinion, based on the language in the Requirement, that the latter assets (Cyber Assets, Virtual Cyber Assets, or SCI) are performing the activity, the current language could be interpreted as indicating the Cyber systems are performing the activity.

Suggested language is as follows:

Cyber systems associated with communication links between assets (Cyber Assets, Virtual Cyber Assets, or SCI) that perform logical isolation that extends to one or more geographic locations.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

Many entities have virtualized systems and were compliant with CIP in recent audits. Please do not over complicate. Focus on security or where gaps exists. Only changes to BCS to include virtual environment and logical asset configuration is required.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Request clarification – is the cyber system equivalent to Cyber Asset? We note that Cyber Asset is a defined term. Cyber system is not a defined term

Request clarification that 4.2.3.2's updates are equivalent to the previous language. Are the demarcation points the same? Explicit exclusions set better expectations.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE recommends defining the term “cyber system.” While it is noted in the technical rationale, the phrase “cyber systems” is not defined in NERC Glossary of Terms. Texas RE recommends defining the term “cyber systems” in the NERC Glossary or, alternatively, use the description provided in the technical rationale to reduce ambiguity in the requirement language. It is unclear whether that undefined term is associated with “system” in CIP CIP-006-7, CIP-007-7, CIP-009-7, CIP-010-5, the “Applicable Systems” column in all CIP standards parts.

Texas RE inquires as to whether these changes would exclude Cyber Assets such as serial/IP converters, data diodes, protocol converters, etc. For example, a serial/IP converter may connect to a BCA serially but convert the protocol from serial to TCP/IP and is connected to a network Cyber Asset that operates at Layer 3 or higher of the OSI model.

Texas RE would recommend providing examples to reduce ambiguity.

Lastly, Texas RE seeks clarification on the phrase “one or more geographic locations.” Registered Entities have a variety of architectural layouts, which could result in confusion regarding the meaning of “one or more geographic locations.” For instance, entities may have two adjacent buildings that could be interpreted as either a single location or separate geographic locations.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

ACES does not agree with the new language. The definition of a Cyber Asset is very clear and well known by the industry. The new language “cyber systems” is not defined and could be interpreted differently by entities and auditors. An Entity can point to specific Cyber Assets easily. We also feel this change was not a part of the FERC order or in the scope of the SAR.

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer	No
Document Name	

Comment

FMPA supports Marty Hostler and Northern California Power Agency comments.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

The change from Cyber Assets to cyber systems could expand this to devices that do not meet the “programable electronic device” portion of the Cyber Asset definition or be interpreted to include a limit on the scope. Cyber systems must be clearly defined.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	No
Document Name	

Comment

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for the CIP-002-5.1a exemption. PG&E does have concerns and supports the input provided by EEI.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

We appreciate the effort to be consistent with the other exemptions. We do not agree that the exemptions for 4.2.3.1, 4.2.3.2 and 4.2.3.3 clearly identify the exempted cyber systems. We believe term “cyber systems” indicates a broader scope than is intended. This could lead to developing each “cyber system” construct that could lead to under or over scoping BES Cyber System assets for CIP-002. We believe that “systems” as used in the other exemptions relates to things that are categorized beyond “cyber systems”. We do recognize “systems” could include cyber systems at these related assets.

Example for 4.2.3.2 & 4.2.3.3: An entity could scope a cyber system as a communication system, where the system would reasonably include substation RTUs, channel banks, digital cross connects, microwave radios, etc. Although in our current version, many entities have included RTUs as BES Cyber Assets, the proposed change would lend to 1) removing RTUs from our CIP Programs or 2) expanding the net to Cyber Assets that have been considered part of the current exception because they are now included as part of the communication system. We realize there are ways around this example, but we wanted to highlight this for the purposes of our discussion.

The exemption language in section 4.2 of every CIP standard will need to be addressed.

For exemption 4.2.3.1 consider removing “cyber” as shown in the following edit:

4.2.3.1. Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

For exemptions 4.2.3.2 & 4.2.3.3, we suggest keeping the exception scope to assets that are defined NERC Glossary terms as shown below:

4.2.3.2. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber Assets, Virtual Cyber Assets and Shared Cyber Infrastructure associated with communication links between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

Also, please provide clarification why the edits included reducing from “communication networks and data communication links” to just “communication links"

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the SRC.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification – is the cyber system equivalent to Cyber Asset? We note that Cyber Asset is a defined term. Cyber system is not a defined term.

Request clarification that 4.2.3.2's updates are equivalent to the previous language. Are the demarcation points the same? Explicit exclusions set better expectations.

Suggest clarification on the geographic locations.

Request clarification – is the cyber system equivalent to Cyber Asset? We note that Cyber Asset is a defined term. Cyber system is not a defined term.

Request clarification that 4.2.3.2's updates are equivalent to the previous language. Are the demarcation points the same? Explicit exclusions set better expectations.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 9.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Neither 4.2.3.2 nor 4.2.3.3 provide a clear understanding of what is exempted because both use terms that are undefined. For 4.2.3.2, the defined term “Cyber Asset” has been replaced by an undefined term “cyber system”. Additionally, the currently approved CIP-002-5.1a exempts communication networks and communication links between discrete ESPs, while the proposed new CIP-002-7 Reliability Standard only exempts the communication links implying that the communications networks may now be subject to CIP Requirements. EEI recommends the restoration of the deleted language to ensure communications networks are exempt from the NERC Standards. Exemption 4.2.3.3 similarly identifies communication links but does not exempt communications networks. This should be corrected. Lastly, the undefined term “logical isolation” is used in both exemptions. As stated in our comments for Question 1, this term should be defined to ensure a clear and common understanding of both the Requirements and Exemptions are contained within the body of CIP Reliability Standards.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy suggests providing clatify to proposed language to provide consistent application.	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	

Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST considers the proposed language of 4.2.3.2 confusing, as it seems to suggest that under certain conditions communications links could provide logical isolation, which is surely not the SDT's intent. N&ST recommends simplifying as follows: "Cyber systems associated with communication links logically isolated from BCS or Shared Cyber Infrastructure (SCI)."	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
The current standard uses "Cyber Asset," which is a defined term. Using "Cyber system" may lead to confusion and inconsistent applicability by using undefined terms. Also, "logical isolation" requires more definition to avoid issues with inconsistency.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	No
Document Name	
Comment	
Two new undefined terms stand out as key concerns in the proposed modifications to the exemptions in CIP-002 (4.2.3.2 and 4.2.3.3): Cyber systems and the concept of logical isolation. "Cyber system" is not defined in the **Glossary of Terms Used in NERC Reliability Standards** (BES Cyber System, yes, but not Cyber system). Nor is there a definition for "logical isolation." Each entity would be required to define these terms. This leaves	

some of the identification of exempted cyber systems (sic) up to the responsible entity and may introduce some areas of dispute between compliance monitoring and entity implementation activity. **Recommendation:** Clarify the term “Cyber systems” and the concept of “logical isolation” so there is a level of consistency across the ERO.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC	
Answer	No
Document Name	
Comment	

Changes made to CIP-002 exemptions noted in 4.2.3.2 and 4.2.3.3 do not provide a clear understanding of what is exempted because both use terms (i.e. cyber systems and logical isolation) which are undefined. Undefined terms need to be defined to ensure a clear and common understanding..	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees to the proposed modifications to split the exemptions into two distinct exemptions to adequately cover all cyber systems associated with conforming changes. Proposed 4.2.3.2 adequately addresses devices outside the identified logical isolation. Proposed 4.2.3.3 may exclude devices providing logical isolation that would otherwise be identified as EACMS. A lack of clarity with respect to the intended scope of this exclusion may result in auditor/entity interperetation disagreements. Assuming the intent is to exclude the connection between the devices, and not the e.g. VPN concentrators themselves, we propose modifying the language to something like "Cyber systems associated with communication links between "logical isolation" provided by Cyber Assets, Virtual Cyber Assets, or SCI where that isolation extends to one or more geographic locations."	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes

Document Name	

Comment

Below is a replication of our response to Question 1, which also addresses this question.

Cyber System (Undefined Term) – Modifications have been made under the exemptions section in CIP-002-7 which move from a Cyber Asset focus to a “cyber system” focus without a corresponding definition of what that term encompasses. With the difficulty of understanding the scope of this undefined term in virtualized environments, Southern recommends developing a definition for “cyber system”, such as:

1. **Cyber System:** *one or more Cyber Assets, VCAs, or SCI used to perform or achieve a cyber-based objective by a Responsible Entity or other party.*

2. Additionally, Southern requests the SDT to consider that Exemption 4.2.3.3. should be a sub-set of Exemption 4.2.3.2. rather than a stand alone item. It appears the main difference between the two exemptions is the distance between the points performing the logical isolation.

• Neither exemptions 4.2.3.2 nor 4.2.3.3 provide a clear understanding of what is exempted, possibly due to the change from “Cyber Asset” to the undefined “Cyber system”. Please see our comments above for a proposed definition of “Cyber System”. Also, the undefined term “logical isolation” is used in both exemptions. As stated in our previous comments, this term should be defined to ensure a clear and common understanding of both the Requirements and Exemptions.

• In order to clearly define exempted cyber systems associated with communication networks, it is necessary for the Registered Entity to clearly designate the communication network components since communication networks, communication systems, or communication assets have no NERC definition. Southern agrees with EEI comments addressing the following recommendations, but clarifying that the second exemption should be a sub-bullet to 4.2.3.2.:

• 4.2.3.2. Cyber systems associated with communication networks, as defined by demarcations set by the Registered Entity, logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

• 4.2.3.2.1 Cyber systems associated with communication networks, as defined by demarcations set by the Registered Entity, between Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that extends to one or more geographic locations.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

BPA feels that the phrase “associated with” a BCS is less than desirable. The concept of “providing connectivity to” or “in the communications chain of but not providing the security controls to” a BCS describes the relationship more clearly.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC supports the splitting of the exemptions to ensure appropriate coverage. However, it respectfully notes that additional clarity could be attained with small tweaks to the proposed exemption language: 4.2.3.2. Cyber systems associated with communication links that meet the following criteria: (1) are logically isolated from BES Cyber Systems or SCI; (2) do not provide logical isolation for BCS or SCI. 4.2.3.3. Cyber systems associated with communication links between Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation beyond one geographic location.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question	

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	

Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

10. BCS and SCI are mutually exclusive by definition, however SCI poses a significant reliability risk to the Bulk Electric System. The SDT considered the risks associated with SCI and revised CIP-002 Requirement R1 to include the identification of SCI in Parts 1.3, 1.4, and 1.5. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC

Answer	No
Document Name	

Comment

Capital Power would like clarification regarding how this proposed change will be applied to low-impact entities. Currently low impact entities are not required to provide a discreet low impact inventory list and the proposed revision seems to contradict this.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO signs on in support of SRC.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	No
Document Name	
Comment	
Conceptually, the SRC agrees with what the SDT has proposed regarding the identification of SCI; however, we don't think the language is clear enough to implement in practice. **Recommendation:** Further clarify the definition to avoid inadvertent inclusion of systems supporting configuration management / monitoring that are not used to implement virtualization; i.e. sharing of computing resources.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
SCI does not present any more risk than EACMS. There is not a specific requirement to identify EACMS, PACS, or PCA in CIP-002. Similarly to EACMS, the association to the BCS is what brings the SCI into scope. SCI should be listed in applicable systems just like EACMS.	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	

Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy believes if there is not a clear understand the concept of SCI and logical Isolation to properly classify Cyber Assets according to function and impact. Need “Logical Isolation” defined.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Same comments to question 11. CIP-002 is the bridge between cybersecurity and reliability function, the inclusion of SCI which is not directly implementing a reliability function does not seem related. Request explicit additional language for (EACMS, PACS, and PCAs) or (remove SCI, EACM, PACS, and PCAs addition). Auditors and entities need clarity on when EACMS, PACS, and PCAs are in scope. Request clarification on R1.5 (Medium Impact). It appears that adding SCI could bring more items into scope. Is that correct? Suggest reviewing the definition for better clarity. Suggest clarification on the analysis required for SCI, SCI/EACMS vs EACMS alone.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the SRC.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

We disagree with the proposed changes. EACMS, PACS and PCAs are not included in the initial CIP-002 process; therefore, the SCI hosting EACMS PACS and PCAs should not be included in the initial CIP-002 process. We recommend revising R1.4 and R1.5as indicated below.

1.4. Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above [delete: or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs)]

1.5. Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above [delete: or their associated EACMS, PACS or PCAs.]

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerns on the definitions caused this no vote for this standard.

Concerned about the use of the term “assets” and the Technical Rationale that states an “asset containing” could be a location of a Management System used to manage a distributed SCI. The TR also includes “control centers” and not “Control Centers”. This could require the inclusion of locations other than the CIP-002 Assets and the location of the device used for electronic security controls, becomes part of the CIP program. Extrapolating this concept out, the entire SCADA system could become part of the program if a portion of it is a BCA.

CIP-002 is the bridge between cyber security and reliability function, the inclusion of SCI which is not directly implementing a reliability function, does not seem related. Request explicit additional language for (EACMS, PACS and PCAs) or (remove SCI, EACM, PACS and PCAs addition). Auditors and entities needs clarity on when EACMS, PACS and PCAs are in scope

Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	
FMPA supports Marty Hostler and Northern California Power Agency comments.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
The definition of Shared Cyber Infrastructure is open to multiple interpretations as written. The confusion is compounded by the exclusion of Shared Cyber Asset from the definition of Cyber Asset (Cyber Asset itself a problematic definition at times). The intent of the SDT is unclear preventing recommending an alternative proposal. NERC, including the SDT, needs to be prepared and ensure that adequate CMEP SDT developed guidance is in place to broadly communicate the intent, implementation guidance, and interpretation of the new definitions on passage and prior to NERC Membership and our vendors beginning work to bring systems into compliance. In general terms, WVPA would have preferred that the SDT adopted the terms and directly adapted the definitions used by NIST in their documentation, such as NIST SP 800-125.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	

Same comments to question 11

CIP-002 is the bridge between cyber security and reliability function, the inclusion of SCI which is not directly implementing a reliability function, does not seem related. Request explicit additional language for (EACMS, PACS and PCAs) or (remove SCI, EACM, PACS and PCAs addition). Auditors and entities needs clarity on when EACMS, PACS and PCAs are in scope

Request clarification on R1.5 (Medium Impact). It appears that adding SCI could bring more items into scope. Is that correct?

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

BCSI requirements are sufficient as in CIP-004 and CIP-011. Entities are compliant and appropriate controls are available to secure BCSI in current version.

Shared storage housing active BCS data should not be allowed for mixed trust environments and introduces significant risk to the BES.

Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based in security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

The language that has been added R1.3, R1.4 and R1.5 is somewhat unclear. Is the intent to identify SCI that hosts BCS, EACMS, PACS, and PCAs, or is the intent to identify SCI that hosts BCS and to identify associated EACMS, PACs, and PCAs? It is not clear what the intent is from the currently proposed language. If the intent is only to identify systems hosted on SCI, then it continues to leave a gap in CIP-002. If the SDT wants to fix the holes in CIP-002, then it should be done correctly and not in pieces, which just compounds the issues. This should be done with a wider view to the breakdowns in how CIP-002 is written so that it improves the security objectives of CIP-002 and how the process of identification of BCS and applicable systems should be identified.

Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Bruce Reimer - Manitoba Hydro - 1	
Answer	No
Document Name	
Comment	
We disagree with these changes. Resulting from our comments for QUESTION 1, SCI is not required because our proposed modifications to the existing definitions can address this issue.	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
More clarification is needed pertaining to what is in scope and what is not in scope?	

As we stated earlier, there is a storage array issue - since storage array wasn't directly impacting assets, this would massively impact Basin - goes against how we have been defining that. PACS on to the storage array - which by these new definitions, implication would need separate storage array for assets that are in scope. Inherent separations are there such as encryption. Need to clearly identify what is contained here.

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

Management Modules are excluded from the definition of SCI, but not explicitly addressed within CAs. The requirements all explicitly address Management Modules of SCI, but not CAs (which should be inherent due to the lack of exclusion in the CA definition). This could lead to entities to exclude required protections for Management Modules on CAs – while implicit within the CA, they are not called out explicitly like in the SCI. Potentially missed requirements would include those around patching, user accounts, logging, change management, etc.

Additionally, for Self-contained Applicaitons defintion:

The term ‘immutable’ may limit the scope of the definition. While the base image may be immutable in a real-time sense, the running container does have the ability to have its configuration changed on an ongoing basis (while still reverting to the image upon termination).

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved:

Management Module

Management Systems

Self-Contained Application

Shared Cyber Infrastructure

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Suggest reviewing the definition for better clarity.

Suggest clarification on the analysis required for SCI, SCI/EACMS vs EACMS alone.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	No
Document Name	

Comment

While CHPD agrees with the identification of SCI, it does not agree with the identification of SCI that host EACMS and PACS unless a corresponding requirement for the identification of EACMS and PACS is created. See question 11.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment	
We disagree with the proposed changes. EACMS, PACS and PCAs are not included in the initial CIP-002 process; therefore, the SCI hosting EACMS PACS and PCAs should not be included in the initial CIP-002 process. We recommend revising R1.4 and R1.5as indicated below. **1.4.** Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above [delete: or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs)] **1.5.** Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above [delete: or their associated EACMS, PACS or PCAs.]	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Suggest reviewing the definition for better clarity. Suggest clarification on the analysis required for SCI, SCI/EACMS vs EACMS alone.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	

Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

We disagree with the proposed changes. EACMS, PACS and PCAs are not included in the initial CIP-002 process; therefore, the SCI hosting EACMS PACS and PCAs should not be included in the initial CIP-002 process. We recommend revising R1.4 and R1.5 as indicated below.

1.4. Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above [**delete: or their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs**)]

1.5. Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above [**delete: or their associated EACMS, PACS or PCAs**.]

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

Comments: *Changes from CIP-002-5.1 to CIP-002-7 include new terminology and applicability, in alignment with virtualization. Part 1.3 was revised to include identification of assets that contain a "low impact BCS and SCI that hosts any portion of a low impact BCS." The new Parts 1.4 & 1.5 added to include identification of associated SCI used for high/med impact BCS, EACMS, PACS or PCA, respectively. Identification of SCI within CIP-002 does address some of the risks associated with virtual infrastructure. However, as with other standards/requirements, CIP-002-7 depends upon approved SCI terminology and other definitions associated with virtualization as a whole.*

Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	

Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
NRG does not agree with the proposed changes. The inclusion of EACMS and PACS as part of the proposed CIP-002 R1.4 and R1.5 is not consistent with the purpose of CIP-002 as a whole. CIP-002 primarily focuses on BES Assets and BES Cyber Systems, not the associated systems. If the intent of these proposed changes is to require an inventory of EACMS, PACS, and PCAs for high and medium impact BCSs, NRG recommends this proposed requirement be moved from CIP-002 to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
Comments: Our comments and recommendations about SCI in QUESTION 1 provides the basis that small modifications to existing definitions can meet the requirement.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	No
Document Name	
Comment	
This is a significant change to a foundational part of the CIP Standards. The SDT is proposing to modify the categorization process from a single step for each asset to a multiple step process of identifying BCS and then reviewing those BCS for associated SCI. Additionally, how does an entity perform this function for low impact SCI when they aren't required to develop a list of low impact BCS?	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
NRG does not agree with the proposed changes. The inclusion of EACMS and PACS as part of the proposed CIP-002 R1.4 and R1.5 is not consistent with the purpose of CIP-002 as a whole. CIP-002 primarily focuses on BES Assets and BES Cyber Systems, not the associated systems. If the intent of these proposed changes is to require an inventory of EACMS, PACS, and PCAs for high and medium impact BCSs, NRG recommends this proposed requirement be moved from CIP-002 to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Comments: Our comments and recommendations about SCI in QUESTION 1 provides the basis that small modifications to existing definitions can meet the requirement.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP is requesting clarification of how the change affects low impact devices	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
This is a significant change to CIP asset accounting. We agree it is a necessary change to help account for virtualization assets. However, identification of SCI should be a result of association to BCS. TVA notes that the risk of a system is based on configuration rather than classification.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	2016-02_Virtualization_Unofficial_Comment_Form_01222021_SC FINAL.docx
Comment	
See attached file.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the identification of SCI in Parts 1.3, 1.4 and 1.5.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 10.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	

Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the approach for BCS and SCI.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	

Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

AEP supports the identification of SCI in CIP-002 Requirement R1 Parts 1.3, 1.4, and 1.5.

Likes 0

Dislikes 0

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed changes.

Likes 0

Dislikes 0

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

Likes 0

Dislikes 0

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC supports the addition and notes the following comments for the SDT's review and consideration:

1. Although the requirements have been modified to be inclusive of SCI and other supporting assets, proposed revisions to the purpose still focus solely on BCS identification. This could lead to confusion and should be revised to comport with the proposed revisions to the requirements. Revisions to the purpose could be as follows:

To identify and categorize cyber systems, assets, and infrastructure for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those that could have on the reliable operation of the BES. Identification and categorization of these systems, assets, and SCI support appropriate protection against compromises that could lead to misoperation or instability in the BES.

2. The format and content utilized for the identification of SCI and associated assets varies between high/medium and low impact BCS. It is recommended that consistent formatting be utilized.

3. In the proposed revisions, it is unclear whether the addition of SCI and attendant systems are those associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., "…hosting [] impact BCS and the BCS's associated ….." or "….hosting [] impact BCS and the SCI's associated….."

4. In the proposed revisions, it is unclear as to whether the intent is to include all of the newly identified assets in the responsible entity's CIP-002 list or whether it is simply an additional identification activity to facilitate overall compliance. Further, the phrasing of the new revisions creates ambiguity relative to what ancillary/supporting assets (EACMS, PACS, and PCAs) are being identified relative. Specifically, the requirements should make clear whether the assets to be identified are:

a. Only the EACMS, PACS, and PCAs associated with SCI;

b. Only the EACMS, PACS, and PCAs associated with BCS AND hosted in SCI;

c. Only the EACMS, PACS, and PCAs associated with BCS that are hosted in SCI;

d. All of the EACMS, PACS, and PCAs associated with BCAs and BCS.

For this reason, clarification is requested. As an example, a revision that reflects option (d) above is provided below.

1.4 Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above or the Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs) associated with the high impact BCS identified in Part 1.1 above.

1.5. Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above or the EACMS, PACS or PCAs associated with the medium impact BCS identified in Part 1.2 above.

5. The VSLs have been revised to incorporate the associated SCI, but not to include the required identification of additional, ancillary assets that are now included in the requirements. Consistency is needed between the requirement verbiage and the VSL verbiage. It is recommended that the revisions to the VSLs be revised to reflect the entirety of the revisions proposed in the requirements or that they be revised to reflect "applicable systems" to avoid the potential for misalignment resulting from revisions.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA suggests that the CIP Senior Manager annually (15 months) review what is included in SCI similarly to reviewing the BCS list for CIP-002 and CIP-003 compliance.	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	

NERC should further clarify what it considers to be Shared Cyber Infrastructure. Additionally, we have a question: is an asset SCI only if it is shared between a non-CIP Applicable System and a CIP Applicable System?

We request clarification on SCI residing at non-BES Facility (for example a data center) which is not a BES asset per those identified in CIP-002 R1 (i) to (vi); need clarification on how we would identify that Facility.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees with the proposed changes.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	
Comment	
The new R1.4 and R1.5 require the identification and categorization of SCI that hosts any portion BCS/EACMS/PACS/PCA. It is agreed that SCI hosting BCS shall be included such that that secure controls/requirements can be properly applied. However, SCI hosting EACMS/PCAS/PCA poses the same risk as the physical EACMS/PCAS/PCA which are not currently included in new CIP-002 requirements. Suggest clarifying that physical EACMS/PCAS/PCA are in scope of CIP-002 or removing the requirements of identifying SCI hosting EACMS/PACS/PCA.	
Likes 0	
Dislikes 0	
Response	

Cynthia Lee - Exelon - 5

Answer

Document Name

Comment

Exelon is aligning with EEI in response to this question.

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon is aligning with EEI in response to this question.

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon is aligning with EEI in response to this question.

Likes 0

Dislikes 0

Response

11. In the current enforceable standards, there are no requirements that can be used to tie a non-identification of EACMS, PACS, and PCAs to a single requirement. The SDT revised CIP-002 to include the identification of SCI associated with EACMS, PACS, and PCAs to help address this issue within the virtualization scope of the current SAR. The proposed requirement could reduce possible non-compliance to a single issue if a Responsible Entity fails to properly identify SCI associated with EACMS, PACS, or PCAs. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Consider revising to include EACMS and PACS as associated systems in the Purpose for consistency. However, identification of EACMS, PACS, and PCAs should be a result of association to BCS.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: Our SCI comments and recommendations in QUESTION 1 support the basis that existng requirements can be slightly modified to meet the SAR and requirments.

Currently there is a gap in CIP-002 that doesn’t require responsible entities to identify EACMS, PACS and PCA, but that aspect is not addressed by this SAR. If SDT intended to resolve this gap, we suggest adding lanaguate to R1.4 in CIP-002-5.1 as follows:

“Identify EACMS, PACS and PCAs that are associated with the high and medium impact BCS.”

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

NRG does not agree with the proposed changes. Please see response to question 10.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Comments: Our SCI comments and recommendations in QUESTION 1 support the basis that existng requirements can be slightly modified to meet the SAR and requirments.

Currently there is a gap in CIP-002 that doesn’t require responsible entities to identify EACMS, PACS and PCA, but that aspect is not addressed by this SAR. If SDT intended to resolve this gap, we suggest adding lanaguate to R1.4 in CIP-002-5.1 as follows:

“Identify EACMS, PACS and PCAs that are associated with the high and medium impact BCS.”

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

ISO-NE agrees with the inclusion of SCI but disagrees with identifying an SCI’s associated systems. CIP-002 is written and designed to identify and categorize systems that impact reliability functions using a bright line criteria. The associated systems, PCA, EACMs, and PACS, are systems used to support security functions that protect the BCS or SCI. The additions also cause confusion because the identification of physical EACMS, PACS, and PCAs was not addressed.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	
Comment	
NRG does not agree with the proposed changes. Please see response to question 10.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Changes from CIP-002-5.1 to CIP-002-7 include new terminology and applicability, in alignment with virtualization. Part 1.3 was revised to include identification of assets that contain a "low impact BCS and SCI that hosts any portion of a low impact BCS." The new Parts 1.4 & 1.5 added to include identification of associated SCI used for high/med impact BCS, EACMS, PACS or PCA, respectively. It clarifies things to make identification of SCI explicit within CIP-002. However, as with other standards/requirements, CIP-002-7 depends upon approved SCI terminology and other definitions associated with virtualization as a whole. Approval of CIP-002-7 would be conditional, based upon approval of the entire suite of new standards associated with virtualization.	
Likes 0	
Dislikes 0	
Response	

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
We disagree with the proposed changes. Virtual EACMS, PACS and PCAs should be identified the same way as physical EACMS, PACS and PCAs. We recommend a future SAR for CIP-002 to address this issue.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
The idea of identifying EACMS, PACS, and PCAs at the level of CIP-002 is interesting, except the VRF should be adjusted to reflect the impact of the asset, i.e., BCS,BCA VRF high EACMS, PACS, and PCAs VRF medium. CIP-002 is based on functional impact on the grid, it’s not obvious to conclude the same impact on the functional impact. Suggest clarification on the requirements.	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We disagree with the proposed changes. Virtual EACMS, PACS and PCAs should be identified the same way as physical EACMS, PACS and PCAs. We recommend a future SAR for CIP-002 to address this issue.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	No
Document Name	

Comment

While CHPD agrees that there is a concern with the current standards' lack of a requirement to identify EACMS, PACS, and PCAs, the identification of such is outside the scope of the SAR. CHPD believes the SDT should not create a two-tiered system where SCI based EACMS and PACS must comply with different requirements than physical ones that are not strictly virtualization based. Such a change should be part of a new SAR.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

The idea of identifying EACMS, PACS, and PCAs at the level of CIP-002 is interesting, except the VRF should be adjusted to reflect the impact of the asset, i.e., BCS,BCA VRF high EACMS, PACS, and PCAs VRF medium.

CIP-002 is based on functional impact on the grid, it's not obvious to conclude the same impact on the functional impact. Suggest clarification on the requirements.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved:

Management Module

Management Systems

Self-Contained Application

Shared Cyber Infrastructure

Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

We disagree with these changes. Resulting from our comments for QUESTION 1, SCI is not required because our proposed modifications to the existing definitions can address this issue. Currently there is a gap in CIP-002 that doesn't require responsible entities to identify EACMS, PACS and PCA, but it is not addressed by this SAR. If SDT intended to resolve this gap, we suggest adding R1.4 to the CIP-002-5.1 as follows:

"Identify EACMS, PACS and PCAs that are associated with the high and medium impact BCS."

Likes 0	
Dislikes 0	

Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
The language that has been added R1.3, R1.4 and R1.5 is somewhat unclear. Is the intent to identify SCI that hosts BCS, EACMS, PACS, and PCAs, or the is the intent to identify SCI that hosts BCS and to identify associated EACMS, PACs, and PCAs? It is not clear what the intent is from the currently proposed language. If the intent is only to identify systems hosted on SCI, then it continues to leave a gap in CIP-002. If the SDT wants to fix the holes in CIP-002, then it should be done correctly and not in pieces, which just compounds the issues. This should be done with a wider view to the breakdowns in how CIP-002 is written so that it improves the security objectives of CIP-002 and how the process of identification of BCS and applicable systems should be identified.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
Based on comments above, these changes are confusing and detrimental to security.	
Likes 0	

Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	

Same comments to question 10

CIP-002 is the bridge between cyber security and reliability function, the inclusion of SCI which is not directly implementing a reliability function, does not seem related. Request explicit additional language for (EACMS, PACS and PCAs) or (remove SCI, EACM, PACS and PCAs addition). Auditors and entities needs clarity on when EACMS, PACS and PCAs are in scope

Request clarification on R1.5 (Medium Impact). It appears that adding SCI could bring more items into scope. Is that correct?

Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	

FMPA supports Marty Hostler and Northern California Power Agency comments.

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

As written, an entity could still be found noncompliant for all requirements applicable to a EACMS, PACS or PCA. This additional requirement seems to add another PNC but only if the EACMS, PACS or PCA is virtualized.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We disagree with the proposed changes. Virtual EACMS, PACS and PCAs should be identified the same way as physical EACMS, PACS and PCAs. We recommend a future SAR for CIP-002 to address this issue.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the SRC.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	

Comment

Same comments to question 10.

CIP-002 is the bridge between cybersecurity and reliability function, the inclusion of SCI which is not directly implementing a reliability function does not seem related. Request explicit additional language for (EACMS, PACS, and PCAs) or (remove SCI, EACM, PACS, and PCAs addition). Auditors and entities need clarity on when EACMS, PACS, and PCAs are in scope.

Request clarification on R1.5 (Medium Impact). It appears that adding SCI could bring more items into scope. Is that correct?

The idea of identifying EACMS, PACS, and PCAs at the level of CIP-002 is interesting, except the VRF should be adjusted to reflect the impact of the asset, i.e., BCS, BCA VRF high EACMS, PACS, and PCAs VRF medium.

CIP-002 is based on functional impact on the grid, it’s not obvious to conclude the same impact on the functional impact. Suggest clarification on the requirements.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

There appears to be a gap in CIP-002 which doesn’t require responsible entities to identify EACMS, PACS and PCA. If SDT intended to resolve this gap, we suggest adding lanaguate to R1.4 in CIP-002-5.1 as follows: “Identify EACMS, PACS and PCAs that are associated with the high and medium impact BCS.”

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1

Answer	No
Document Name	

Comment

Please see JEA coments, an individual response to my comment is not required.

Likes 0	

Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
SCI does not present any more risk than EACMS. There is not a specific requirement to identify EACMS, PACS, or PCA in CIP-002. Similarly to EACMS, the association to the BCS is what brings the SCI into scope. SCI should be listed in applicable systems just like EACMS.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	No
Document Name	
Comment	
Conceptually, the SRC supports what the SDT is attempting to do regarding the consolidation of requirements to identify EACMS, PACS and PCAs into a single requirement. CIP-002 should include requirement language specific to the identification of any necessary categories to support the use of the Applicable Systems specification throughout the rest of the CIP standards. To do otherwise introduces a potential gap in activity required to identify and protect critical infrastructure and the systems supporting such protection.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	

Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the proposed modifications. However, the proposed modification only seems to solve the problem for SCI and not existing issues with associated Cyber Assets. Duke Energy is concerned that the treatment of SCI in a manner not commensurate with other in-scope systems introduces discrepancies in enforcement methods that will present challenges in working with regions. The current SAR should be expanded to address inventories of all relevant devices.	
Likes 0	
Dislikes 0	

Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
The modifications could reduce possible non-compliance to a single issue.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the SDT's intent to tie a non-identification of EACMS, PACS, and PCAs to a single requirement; however, Southern questions the usefulness in performing this activity only on virtual versions of these assets hosted on SCI that are being proposed for addition to CIP-002-7. Would physical Cyber Assets performing EACMS, PACS, or PCA functions not be just as important to identify and include? If the challenge of also including physical Cyber Assets alongside virtual ones in CIP-002 is a result of the scoping of the existing virtualization SAR, then… well, that is a shame and a gap in the ROP that should be addressed.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	

Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

In the proposed revisions, it is unclear as to whether the intent is to include all of the newly identified assets in the responsible entity's CIP-002 list or whether it is simply an additional identification activity to facilitate overall compliance. Further, the phrasing of the new revisions creates ambiguity relative to what ancillary/supporting assets (EACMS, PACS, and PCAs) are being identified relative. Specifically, the requirements should make clear whether the assets to be identified are:

a. Only the EACMS, PACS, and PCAs associated with SCI;

b. Only the EACMS, PACS, and PCAs associated with BCS AND hosted in SCI;

c. Only the EACMS, PACS, and PCAs associated with BCS that are hosted in SCI;

d. All of the EACMS, PACS, and PCAs associated with BCAs and BCS.

For this reason, clarification is requested. As an example, a revision that reflects option (d) above is provided below.

1.4 Identify associated SCI that hosts any portion of the high impact BCS identified in Part 1.1 above or the Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs) associated with the high impact BCS identified in Part 1.1 above.

1.5. Identify associated SCI that hosts any portion of the medium impact BCS identified in Part 1.2 above or the EACMS, PACS or PCAs associated with the medium impact BCS identified in Part 1.2 above.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	

Portland General Electric Company supports this change

Likes 0	

Dislikes 0

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

Likes 0

Dislikes 0

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed changes.

Likes 0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer	Yes
Document Name	

Comment

AEP supports the revisions to CIP-002 that include the identification of SCI associated with EACMS, PACS, and PCAs.

Likes 0

Dislikes 0

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	

Answer	Yes
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	Yes
Document Name	

Comment

Texas RE agrees with the proposed changes. Additionally, although not specifically related to virtualization, it recommends the identification of all EACMS, PACS, and PCAs be required. If the identification of EACMS, PACS, or PCAs is only required for SCI, there is still "*no requirements that can be used to tie a non-identification of EACMS, PACS, and PCAs to a single requirement*" for EACMS, PACS or PCAs not associated with SCI. Texas RE recommends the following language:

- Identify each of the high impact BCS according to Attachment 1, Section 1, if any, at each asset; and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).
- Identify each of the medium impact BCS according to Attachment 1, Section 1, if any, at each asset; and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).

Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the approach for the identification of SCI associated with EACMS, PACS, or PCA.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 11.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the revisions to CIP-002 that include the identification of SCI associated with EACMS, PACS, and PCAs.	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	
Comment	
See comments in Q10	

Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	

12. The SDT modified CIP-002 Attachment 1, Criterion 2.1 to align with a previously approved Request for Interpretation (RFI) regarding “shared BES Cyber Systems.” The SDT modified the criterion to reference each discrete shared BCS. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1

Answer	No
Document Name	

Comment

Please see JEA coments, an individual response to my comment is not required.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

CPS Energy believes changes should be made to Criterion 2.1 and 2.2

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the SRC.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We agree with this change; however, the qualifier of “at a single plant location” should be added. 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units [insert: **at a single plant location**], the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Request clarification - could multiple virtualized Low Impact BCS sharing the same SCI make that SCI Medium Impact under Criterion 2.1?	
Likes 0	
Dislikes 0	

Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based in security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
The language needs to make it more clear that the individual BCS would have to be in support of the generating units that surpass the threshold. The language change doesn't seem to clarify the interpretation of the criteria over the previous language that was used.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	

Response

Bruce Reimer - Manitoba Hydro - 1

Answer	No
Document Name	

Comment

See attachment for comments.

Likes 0	
Dislikes 0	

Response

Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6

Answer	No
Document Name	

Comment

CIP-002 Attachment 1, Criterion 2.1 is poorly worded.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved:

Management Module

Management Systems

Self-Contained Application

Shared Cyber Infrastructure	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with this change; however, the qualifier of “at a single plant location” should be added. 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units [insert: **at a single plant location**], the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	

We agree with this change; however, the qualifier of “at a single plant location” should be added.

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units [insert: **at a single plant location**], the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6

Answer	No
Document Name	

Comment

Request clarification: could multiple virtualized low impact BCS sharing the same SCI make that SCI medium impact under R2.1.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No

Document Name	
Comment	

Comments: We believe adding "discrete" in Criterion 2.1 does not resolve the clarification. Criterion 2.1 and 2.2 have the same issue regarding which shared BCS shoulde be identified as medium impact.

In our view, the focus should be on a totol loss of 1500MWs or 1000MVAR rather than the adverse impacts. If using adverse impact as the assessment basis, all BCS would be identified as the medium impact BCS. In addition, the "shared" wording should be removed since non-shared BCS could also result in a loss of 1500MW.

Recommendations:

Changes to the Criterion 2.1 and 2.2 to be:

- 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. An individual BCS for a group of generating units, that could, within 15 minutes result in a total loss of 1500 MW or more in a single Interconnection.

Likes 0	
Dislikes 0	
Response	

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	
Comment	

Comments: We believe adding "discrete" in Criterion 2.1 does not resolve the clarification. Criterion 2.1 and 2.2 have the same issue regarding which shared BCS shoulde be identified as medium impact.

In our view, the focus should be on a total loss of 1500MWs or 1000MVAR rather than the adverse impacts. If using adverse impact as the assessment basis, all BCS would be identified as the medium impact BCS. In addition, the "shared" wording should be removed since non-shared BCS could also result in a loss of 1500MW.

Recommend:

Changes to the Criterion 2.1 and 2.2 to be:

- 2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. An individual BCS for a group of generating units, that could, within 15 minutes result in a total loss of 1500 MW or more in a single Interconnection.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the change made to CIP-002 Attachment 1, Criterion 2.1 to address the approved RFI regarding “shared BES Cyber Systems”.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 12.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes

Document Name	
Comment	
Request clarification - could multiple virtualized Low Impact BCS sharing the same SCI make that SCI Medium Impact under Criterion 2.1? The syntax should be the same for Criterion 2.2. Criterion 2.1 is the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, The current Criterion 2.2 is the only BCS that meet this criterion are those shared BCS that could, within 15 minutes.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the inclusion of the earlier CIP-002-5.1a imterpertation into CIP-002, Attachment 1, Criteria 2.1.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE notes that Part 2.12 was not approved by FERC and needs to be adjusted to the language found in CIP-002-5.1a.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes

Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
LCRA believes that having the “each discrete” before “shared BES Cyber Systems” sounds contradictory and may lead to confusion.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

AEP supports the change made to CIP-002 Attachment 1, Criterion 2.1 to address “shared BES Cyber Systems”.

Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
LCRA believes that having the “each discrete” before “shared BES Cyber Systems” sounds contradictory and may lead to confusion.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	Yes
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

The syntax should be the same for Criterion 2.2. and Criterion 2.1..

Criterion 2.1. is :

the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes,

The current Criterion 2.2 is :

The only BCS that meet this criterion are those shared BCS that could, within 15 minutes,

Likes 0	
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	Yes

Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Yes, Southern supports this change to CIP-002-6, Att 1, Part 2.1 criteria.	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

SRP is requestiong futher definition, “each discrete shared” BCS mean within the standard.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

The added term "discrete" helps to clarify what should be taken into account to calculate the 15-minute impact.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy generally agrees with the proposed modifications to align with a previously approved Request for Interpretation (RFI) regarding shared BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	
Document Name	
Comment	
The SRC defers to comment as this Criterion is not applicable to the ISO/RTO community.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
Please see comments submitted by the ISO/RTO Council Standards Review Committee.	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	

Answer	
Document Name	

Comment

Abstain, not applicable to medium impact.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	
Document Name	

Comment

Please see comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment
Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response
Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment
Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

13. The SDT made conforming changes to CIP-003 and CIP-004. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

TVA disagrees with the underlying changes that necessitate the conforming changes.

Likes 0	
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP considers the attention given to virtualization feels over weighted compared to non-virtualized systems. This increases the burden on entities without virtualization to comb through the standards to find what is applicable.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: Our comments and recommendations in QUESTION 1 address CIP-003 and CIP-004. Based on our proposed revision to the definition of IRA, we agree the applicable systems in CIP-004 should be changed from “medium impact BCS with ERC to “medium impact BCS with ERC or IRA.”

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

CIP-003 Attachment 1 states, “Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS or their associated SCI.” Please verify the usage of and/or in this sentence. Could an entity have a plan for either the BCS or associated SCI or do they need a plan for both, if applicable? The intent is not difficult to infer, but the SDT could clarify the intent with revised language.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Comments: Our comments and recommendations in QUESTION 1 address CIP-003 and CIP-004. Based on our proposed revision to the definition of IRA, we agree the applicable systems in CIP-004 should be changed from “medium impact BCS with ERC to “medium impact BCS with ERC or IRA.”

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Agreement depends upon approved SCI terminology and other definitions associated with virtualization as a whole and documented throughout our comments.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Suggest a definition of « the **system(s)** outside the asset containing low impact BES Cyber System(s)BCS » a requirement 3.1 section 3 of the attachment 1 in CIP-003.	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We agree with the conforming changes to CIP-003 and CIP-004 Standard language.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1

Answer	No
Document Name	

Comment

In relation to CIP-004 R2.1, the new definition of IRA and addition of IRA to this requirement will expand the scope to serially connected assets that have IRA, which has a significant impact due to the large number of BC Hydro assets which are Medium Impact without ERC.

BC Hydro SME team suggests that SDT either revise the IRA definition and include routing as suggested in our response to Question # 1, or restore the previous version of the standard for this requirement with newly added terms.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Suggest reviewing the definition for better clarity.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

CIP-003 and CIP-004

Some of the proposed new terms (listed below) are ambiguous and arbitrary. Additional clarification and contextually relevant guidance is needed to better articulate the meaning of such Terms. For example, technical diagrams, examples of cyber assets, or infrastructure scenarios would be beneficial, before the standards are approved:

Management Module

Management Systems

Self-Contained Application

Shared Cyber Infrastructure

CIP-004

Comment: The change to this requirement would include all of the Medium Impact BCS.

However, additional clarity is needed on the new terms to see how this requirement affects an entity's facility that contain Medium Impact BCS.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

See MEC and BHE comments.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

The term “system(s)” in R2, Atch. 1, sections 3.1 is unclear whether itvrefers only to Cyber Assets and Virtual Cyber Assets. Would this term also include SCI? Since the Technical Rationale for Atch 1 Section 3.1 is the only place that describes the term “system(s)”, future revisions of the Technical Rationale should retain the description if still applicable. For clarity, the term "system" should be defined in the language of the requirement itself if it is intended to be applicable only to this instance of the usage of the term.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

Current standards are sufficient and these changes are cosmetic. No changes to CIP-004 are required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Without further refinement to the requirements as discussed in answers to the other questions, it would be inappropriate to support this change to the applicability

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE is concerned security risks still exist for CIP-004-7 by not including PCAs in the applicable systems column specifically for R4 and R5.

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer	No
Document Name	

Comment

FMPA supports TVA's comments.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerns on the definitions caused this no vote for this standard.

ESP is still included in CIP-003 R1.1.2 even though it is retired. Should be replaced with the new name of CIP-005.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We agree with the conforming changes to CIP-003 and CIP-004 Standard language. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Eenrgy belives changes the applicable systems should be “medium impact BCS with ERC or IRA.” for CIP-004.	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	

Please see JEA coments, an individual response to my comment is not required.

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5

Answer	No
Document Name	

Comment

We don’t agree with adding IRA as it will bring into compliance more devices that were previously excluded.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

Please see comments in response to Question No. 9 regarding exemptions 4.2.3.2 & 4.2.3.3.

Likes 0	
Dislikes 0	

Response

Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC

Answer	No
Document Name	

Comment

CIP-003 Attachment 1 states, “Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS or their associated SCI.” Please verify the usage of ’or’ in this sentence. Could an entity have a plan for either the BCS or associated SCI or do they need a plan for both, if applicable? The intent is not difficult to infer, but the SDT could clarify the intent with revised language.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy generally agrees with the conforming changes to CIP-003 and CIP-004.	

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	Yes
Document Name	

Comment

Reclamation recommends changing the title of CIP-003-9 Attachment 1

From: Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS or their associated SCI

To: Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS and associated SCI

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern supports the conforming changes made to CIP-003 and CIP-004 given that the SDT is able to adequately address our other comments contained herein.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	Yes
Document Name	

Comment

We agree with the conforming changes to CIP-003 and CIP-004.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC provides the following comments on the conforming changes to CIP-003 and CIP-004 for the SDT's review and consideration:

2. The introductory sentence for CIP-003, requirement R1 was revised to include "and associated SCI," however, the applicable bullets in the subset list still only address BCS. While not all topics are applicable to SCI, several are and, therefore, the singular reference to BCS in a sub-bullet could result in confusion and ambiguity relative to whether the policy should address SCI relative to that topic. For example, requirements R1.1.3 and R1.1.6 address topics that are also applicable to SCI, but include only references to BCS. The SDT should clarify as to whether content on these topics should address solely BCS or also SCI and give due consideration as to how these similarities and differences in treatment of BCS and SCI should be addressed in Requirement R1.

3. Requirement R1.1.2 in CIP-003 still refers to ESPs despite the proposal to retire the term included in this posting.

4. The proposed revisions include modifications to the titles of certain reliability standards, e.g., CIP-005 and CIP-010, and titles should be modified in others to reflect the expanded scopes (e.g., inclusion of SCI), e.g., CIP-006 and CIP-009. Several of the bullets included in requirement R1 do not reflect the revised titles. Accordingly, a quality check should be performed to ensure consistency between CIP-003 and the referenced CIP reliability standard’s titles with conforming revisions proposed where necessary. Alternatively, the topics could be revised to ensure broader applicability.

5. In the proposed revisions for CIP-004, for applicable systems, it is unclear why the construct/format utilized differs between requirements, e.g., requirement R1 and R2, and whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI

or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., "…hosting [] impact BCS and the BCS's associated ….." or "….hosting [] impact BCS and the SCI's associated….."

6. In the applicable systems column, the reference to SCI includes an "or" and not an "and." This creates uncertainty as to whether both "their associated EACMS or PACS" must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are "and" focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

It seems unneccesary to call out SCI in applicable systems column of CIP-004 R1.1 as other associated systems are not called out in the awareness training. There does not appear to be any real value gained by adding this qualifier to this section.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed conforming changes to CIP-003 and CIP-004.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP generally supports the conforming changes made to CIP-003 and CIP-004, except for those concerns identified within our responses to Questions 1 and 9.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	

AEPCO is signing on to ACES comments.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	Yes
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Issue 1:

The addition of “with IRA” to the Applicable Systems column in CIP-004 will add significant burden to authorize and revoke access to systems that were previously not required to be managed in this way under CIP-004. There are many instances of medium impact facilities that have their external communication limited to serial in order to limit risk, which had the added benefit of de-scoping many CIP Requirements (CIP-004 being one set).

Issue 2:

Tacoma Power noted the lack of Management Module inclusion in the Applicability column in CIP-004, and would like feedback from the SDT on whether this exclusion was intentional.

Issue 3:

Additionally, the Applicable Systems SCI references in CIP-004 R5 should be sub-bulleted. For example, “SCI hosting High Impact BCS or their associated EACMS or PACS” should be changed to “•EACMS” and “•PACS”.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change.	

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-003 and CIP-004. PG&E does have concerns and supports the input provided by EEI.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	Yes
Document Name	

Comment

Suggest reviewing the definition for better clarity.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb

Answer	Yes
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 13.

Likes 0	

Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI generally supports the conforming changes made to CIP-003 and CIP-004, except for those concerns identified within our responses to Questions 1 and 9.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	Yes
Document Name	
Comment	
The SRC supports the conforming changes made to CIP-003 and CIP-004 with respect to the high impact provisions applicable to ISO/RTO functions.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	
Document Name	

Comment

Please see comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

14. The SDT modified the Applicable Systems column in CIP-006 to include SCI hosting PACs associated with Medium Impact BCS with ERC or IRA. The SDT made the proposed revisions to clarify the scope of requirements that apply when an entity implements serial IRA. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

The changes appear to be appropriate as long as corrections are made to the SCI definition. In addition, please see comments in response to Question No. 9 regarding exemptions 4.2.3.2 & 4.2.3.3.

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1

Answer	No
Document Name	

Comment

Please see JEA coments, an individual response to my comment is not required.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	

Comment

R2.2 – Request removal of “except during CIP Exceptional Circumstances” from R2.2. See the requirement column. This language was moved to R2. So, this exception already applies to this Part.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - Trevor Tidwell - 1,3

Answer	No
Document Name	

Comment

No we disagree. In fact we don't even understand the questions based on the reading of the standard. So what ever the drafting team was trying to communicate isn't being conveyed in the current draft. What is the risk that this change is trying to address? Additionally, we agree with submitted comments from Duke Energy regarding the mention of serial IRA.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

CPS Eenrgy belives changes the applicable systems should be “medium impact BCS with ERC or IRA.” for CIP-006 and suggests providing clatify to proposed language to provide consistent application.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI recognizes the clear linkage between SCI hosting PACs associated with Medium Impact BCS with ERC within CIP-006, but there seems to be a gap in that linkage for IRA. Presently, IRA is not mentioned within the language of proposed CIP-006-7 or the technical rationale. EEI requests clarification how serial IRA is to be addressed within the framework of CIP-006-7 without clear linkage to IRA. At the present time, the only references to serial IRA are within the Technical Rationale for Definitions (see IRA). For this reason, EEI is unable to support the proposed changes.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 14.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

R2.2 – Request removal of “except during CIP Exceptional Circumstances” from R2.2. See the requirement column. This language was moved to R2. So, this exception already applies to this Part.

Likes 0	

Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We disagree with the proposed changes to CIP-006. The present changes do not reference IRA within the language of proposed CIP-006-7 or the Technical Rationale. We request clarification on how the serial IRA is to be addressed within the framework of CIP-006-7 without clear linkage to the IRA. Presently, only references to serial IRA are within the Technical Rationale for Definitions. Additionally, more information in the Technical Rationale is requested regarding the concept and procedural controls of SCI without ERC hosting Medium Impact BCS, as found in the Applicable Systems of R1 part 1.1.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard. Do not understand how the proposed changes in scope have any impact on serial IRA. This clarification of scope does not seem to be discussed in the Technical Rational for CIP-006.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	No
Document Name	
Comment	

Portland General Electric Company supports the comments provided by EEI for this survey question.

Likes 0	
Dislikes 0	

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer	No
Document Name	

Comment

FMPA supports TVA's comments.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Without further refinement to the requirements as discussed in answers to the other questions, it would be inappropriate to support this change to the applicability

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren agrees with and supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Becky Webb - Exelon - 6

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP, in support of EEI’s comments, recognizes the clear linkage between SCI hosting PACs associated with Medium Impact BCS with ERC within CIP-006, but there seems to be a gap in that linkage for IRA. Presently, IRA is not mentioned within the language of proposed CIP-006-7 or the Technical Rationale. AEP requests clarification on how serial IRA is to be addressed within the framework of CIP-006-7 without clear linkage to IRA. At the present time, the only references to serial IRA are within the Technical Rationale for Definitions (see IRA). For this reason, AEP is unable to support the proposed changes.

Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
“SCI hosting PACs associated with Medium Impact BCS with ERC or IRA” is not in the Applicable Systems column for any of the CIP-006 requirements. Otherwise, SIGE agrees that serial IRA should be in scope.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	

Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
"SCI hosting PACs associated with Medium Impact BCS with ERC or IRA" is not in the Applicable Systems column for any of the CIP-006 requirements. Otherwise, CEHE agrees that serial IRA should be in scope.	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
More information is needed on storage requirements and scope needs to be defined. SCI considerations will dictate our agreement to this particular item.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Medium Impact BCS with ERC or IRA is not listed in the Applicable Systems column in CIP-006-7. The question does not reflect the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
We support the NPCC TFIST and RSC comments and submit the following additional comments: R2.2 – Request removal of “except during CIP Exceptional Circumstances” from R2.2. See the requirement column. This language was moved to R2. So, this exception already applies to this Part	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	No
Document Name	
Comment	
Similar to comments provided in our response to Question # 1, the change in the definition of IRA and the use of term “Medium Impact BCS with ERC or IRA” will result in a major scope increase and change for BC Hydro. BC Hydro SME team suggests that SDT either revise the IRA definition and include routing as suggested in our response to Question # 1, or restore the previous version of standard for this requirement with newly added terms.	

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We disagree with the proposed changes to CIP-006. The present changes do not reference IRA within the language of proposed CIP-006-7 or the Technical Rationale. We request clarification on how the serial IRA is to be addressed within the framework of CIP-006-7 without clear linkage to the IRA. Presently, only references to serial IRA are within the Technical Rationale for Definitions. Additionally, more information in the Technical Rationale is requested regarding the concept and procedural controls of SCI without ERC hosting Medium Impact BCS, as found in the Applicable Systems of R1 part 1.1.

Likes 0	
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question

Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
R2.2 – Request removal of “except during CIP Exceptional Circumstances” from R2.2. See the requirement column. This language was moved to R2. So, this exception already applies to this Part	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
We disagree with the proposed changes to CIP-006. The present changes do not reference IRA within the language of proposed CIP-006-7 or the Technical Rationale. We request clarification on how the serial IRA is to be addressed within the framework of CIP-006-7 without clear linkage to the IRA. Presently, only references to serial IRA are within the Technical Rationale for Definitions. Additionally, more information in the Technical Rationale	

is requested regarding the concept and procedural controls of SCI without ERC hosting Medium Impact BCS, as found in the Applicable Systems of R1 part 1.1.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

NRG does not agree that the proposed revisions clarify the scope of requirements with respect to IRA. Specifically, none of the “Applicable Systems” columns throughout CIP-006 contain the verbiage, “IRA”.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

ISO-NE disagrees with the addition of “SCI hosting High Impact BCS or their associated EACMS or PCA” and “SCI with ERC hosting Medium Impact BCS or their associated EACMs or PCA” to the applicable systems for CIP-006 R1.6 and CIP-006 R1.7. These additions are in conflict with the requirements language that focuses on the protections to Physical Access Control Systems themselves. Excerpt of Requirement Language for context. CIP-006 R1.6 “Monitor each Physical Access Control System for unauthorized physical access to a **Physical Access Control System**.” CIP-006 R1.7 “Issue an alarm or alert in response to detected unauthorized physical access to a **Physical Access Control System** to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.” ISO-NE agrees with the addition of “SCI hosting PACS associated with High Impact BCS” and “SCI hosting PACS associated with Medium impact BCS with ERC” as this correctly reflects the intention of the requirements.	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
Document Name	
Comment	
No response, however refer to previous need for IRA change clarification	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
Comments: Our comments and recommendations in QUESTION 1 address CIP-006. Based on our proposed IRA revision, we believe the applicable systems in CIP-006 should be changed from medium impact BCS with ERC to “medium impact BCS with ERC or IRA.”	
Likes 0	

Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
The applicability section does not clarify the scope of requirements that apply when an entity implements serial IRA in CIP-006. It clearly defines the scope for BCS and SCI with ERC.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
NRG does not agree that the proposed revisions clarify the scope of requirements with respect to IRA. Specifically, none of the “Applicable Systems” columns throughout CIP-006 contain the verbiage, “IRA”.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Comments: Our comments and recommendations in QUESTION 1 address CIP-006. Based on our proposed IRA revision, we believe the applicable systems in CIP-006 should be changed from medium impact BCS with ERC to “medium impact BCS with ERC or IRA.”	
Likes 1	Lincoln Electric System, 1, Johnson Josh

Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The undefined term "serial IRA" appears to be in conflict with the current definition of IRA supplied in the NERC Glossary of Terms. Remove "serial," or clarify what is meant by "serial IRA." The proposed language lacks the clarity to provide a consistent application.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not agree that the proposed modifications clarify the scope of requirements that apply when an entity implements serial IRA. There is no inclusion of IRA within the language of proposed CIP-006-7 or the technical rationale. Duke Energy recommends clarification as to how serial IRA are to be addressed within the framework of CIP-006-7.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-006 to include SCI. PG&E does have concerns and supports the input provided by EEI.

Likes 0	
Dislikes 0	

Response
Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	Yes
Document Name	

Comment
Texas RE does not have comments on this question.

Likes 0	
Dislikes 0	

Response
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	Yes
Document Name	

Comment
AEPCO is signing on to ACES comments.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed changes.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC provides the following comments for the SDT's review and consideration:

7. It is recommended that the SDT evaluate whether revisions to the title and purpose of CIP-006 are necessary to ensure consistency with its expanded scope.

8. In the applicable systems column, the reference to SCI includes an "or" and not an "and." This creates uncertainty as to whether both "their associated EACMS or PACS" must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are "and" focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

If the SDT specifically meant to address IRA, then it was not achieved. We do NOT see any reference to the term Interactive Remote Access or IRA in the proposed standard.

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Adding “SCI Hosting High Impact BCS” and “SCI with ERC Hosting Medium Impact BCS” is necessary to insure that the scope of the applicable systems includes any possible virtual systems.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern acknowledges the clear linkage between SCI hosting PACs associated with Medium Impact BCS with ERC within CIP-006, but there seems to be a typo in this question related to IRA. Presently, IRA is not mentioned within the language of proposed CIP-006-7, as a qualifier for any Applicable System, or mentioned in the Technical Rationale. Southern recommends clarification as to how the implementation of serial IRA is to be addressed within the framework of CIP-006-7. Otherwise, Southern supports the ability to place the physical underlay of SCI hosting PACS associated with h/m BCS with ERC inside a PSP to meet the requirement.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	

Agree, with the proposed change to clarify the scope of the requirements for applicable systems with ERC and without ERC, but none of the applicable systems in CIP-006 included any reference to IRA as the question suggests.

Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	

Answer

Document Name

Comment

Conceptually, the SRC agrees with what the SDT is proposing to do; however, we defer to medium and low impact entities to comment on the proposed language.

Likes 0

Dislikes 0

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer

Document Name

Comment

Please see comments submitted by the Edison Electric Institute

Likes 0

Dislikes 0

Response

Cynthia Lee - Exelon - 5

Answer

Document Name

Comment

Exelon is aligning with EEI in response to this question.

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

15. The SDT made conforming changes to CIP-008 and CIP-009. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
TVA disagrees with the underlying changes that necessitate the conforming changes.	
Likes 0	
Dislikes 0	
Response	

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP considers the attention given to virtualization feels over weighted compared to non-virtualized systems. This increases the burden on entities without virtualization to comb through the standards to find what is applicable.	
Likes 0	
Dislikes 0	
Response	

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Comments: Our comments and recommendations in QUESTION 1 address CIP-008 and CIP-009 regarding the new or modified definitions.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
Comments: Our comments and recommendations in QUESTION 1 address CIP-008 and CIP-009 regarding the new or modified definitions.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Agreement depends upon approved SCI terminology and other definitions associated with virtualization as a whole and documented throughout our comments.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	

Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with the conforming changes to CIP-008 and CIP-009 in the Standard language. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Until more context (technical diagrams or examples of applicable cyber assets) is provided for the SCI definition.	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	

Answer	No
Document Name	
Comment	
Agree with changes to CIP 009. For CIP 008, scope needs to be limited to only include devices that impact the BES.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Without further refinement to the requirements as discussed in answers to the other questions, it would be inappropriate to support this change to the applicability	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	

Comment	
FMPA supports TVA's comments.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We agree with the conforming changes to CIP-008 and CIP-009 in the Standard language. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	

Comment	
CPS Energy believes the attention given to virtualization feels over weighted compared to non-virtualized systems and may increase burden to entities.	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
The changes appear to be appropriate as long as corrections are made to the SCI definition. In addition, please see comments in response to Question No. 9 regarding exemptions 4.2.3.2 & 4.2.3.3.	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	

Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees to the conforming changes to CIP-008 and CIP-009.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the conforming changes made to CIP-008 and CIP-009 given that the SDT is able to adequately address our other comments contained herein.	
Likes 0	

Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
We agree with the conforming changes to CIP-008 and CIP-009.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Suggest reviewing the definition for better clarity.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	

Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
In the proposed revisions for CIP-008 and CIP-009, for applicable systems, it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these across the body of CIP reliability Standards along with attendant revisions for clarity are requested e.g., "…hosting [] impact BCS and the BCS's associated …..." or "….hosting [] impact BCS and the SCI's associated….." Further, in the applicable systems column, the reference to SCI includes an "or" and not an "and." This creates uncertainty as to whether both "their associated EACMS or PACS" must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are "and" focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	

We support the NPCC TFIST and RSC comments and submit the following additional comments:

Suggest reviewing the definition for better clarity.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

MPC supports comments submitted by Duke Energy.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed conforming changes to CIP-008 and CIP-009.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	Yes
Document Name	

Comment

AEP generally supports the conforming changes made to CIP-008 and CIP-009, except for those concerns identified within our responses to Questions 1 and 9.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	

Tacoma Power recommends that the SDT add a note in the CIP-008-7 technical rationale to capture definition changes to “Cyber Security Incident” and “Reportable Cyber Security Incident”.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE does not have comments on this question.	

Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and generally agrees with the approach for CIP-008 and CIP-006. PG&E does have concerns and supports the input provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Suggest reviewing the definition for better clarity.	
Likes 0	

Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 15.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI generally supports the conforming changes made to CIP-008 and CIP-009, except for those concerns identified within our responses to Questions 1 and 9.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	Yes
Document Name	
Comment	
Other than the concerns noted in our response to Question #9, the SRC supports the conforming changes made to CIP-008 and CIP-009.	
Likes 0	
Dislikes 0	

Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0

Dislikes 0

Response

Cynthia Lee - Exelon - 5

Answer

Document Name

Comment

Exelon is aligning with EEI in response to this question.

Likes 0

Dislikes 0

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer

Document Name

Comment

Please see comments submitted by the Edison Electric Institute

Likes 0

Dislikes 0

Response

Dania Colon - Orlando Utilities Commission - 5

Answer

Document Name

Comment

Current standards are sufficient and these changes are cosmetic. No changes to CIP-008 or 009 are required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

Likes 0	
Dislikes 0	
Response	

16. The SDT modified CIP-011 Requirement R2 part 2.1, which will allow cryptographic erasure in scenarios where BCSI can't be mapped to particular disks in virtualized storage. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

CAISO signs on in support of SRC.

Likes 0	
Dislikes 0	

Response

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization

Answer	No
Document Name	

Comment

The SRC agrees with combining Parts 2.1 and 2.2 under Requirement R2 and proposes to augment the proposed language by adding "that contain BCSI" as some BES Cyber Assets, such as PCA, may not contain BCSI at all.

Recommendation: Revise the Requirement in Part 2.1 as follows:

Method(s) to prevent the unauthorized retrieval of BCSI from applicable systems ***that contain BCSI*** *prior to their disposal or reuse (except for reuse within other systems identified in the "Applicable Systems" column).*

Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
CIP-011 Part 2.1 does not mention cryptographic erasure. It is unclear what is meant by “cryptographic erasure.” It would be more appropriate for the SDT to directly address striping of data or other means that obfuscate information on disks in virtual storage. The second requirement is identified as R1. It should be R2.	
Likes 0	
Dislikes 0	
Response	
Aaron Staley - Orlando Utilities Commission - 1	
Answer	No
Document Name	
Comment	
Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Gladys DeLaO - CPS Energy - 1	
Answer	No
Document Name	
Comment	
Although cryptographic erasure (CE) is utilized making the encrypted data impossible to decrypt, is it possible to recover data (BCSI) from the applicable system since there was no specifc data targeted? Additionally, consider revising the new part 2.1: “Method(s) to prevent the unauthorized	

retrieval of BCSI from applicable systems that contain BCSI prior to upon their disposal or reuse (except for reuse within other systems identified in the “Applicable Systems” column). “

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request correct label for R2. Currently shows R1 – immediately before M2 – on PDF page 9 of 18.

Request review of the column Applicable Systems, Management modules, and Management systems should be part of R1 and R2.

Request clarification in the requirement to allow cryptographic erasure, this mechanism should not be in the requirement, the requirement should stay at the high level. cryptographic erasure should me move to the Technical Rationale.

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the SRC.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No

Document Name	
Comment	
We agree with the proposed changes to CIP-011 R2 part 2.1. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP offers the following comment for the SDT consideration for Question 16: Recommend the SDT add clarity to the requirement or measure on the reuse of the physical storage location of virtual machine files being deleted or removed from the SCI. This could become problematic to machines that reside outside the ESP (EACMS and PACS).	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Concerns on the definitions caused this no vote for this standard.	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	

Answer	No
Document Name	

Comment

FMPA supports TVA's comment: Consider revising to include a process to capture the encryption keys' management if using VMs/solid-state drives. The proposed language does not include the term "cryptographic erasure". The proposed language lacks the clarity to provide the consistent application.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	No
Document Name	

Comment

The Measures section stating “Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI” should be extended to allow escorted transport between physical security perimeters.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

Request correct label for R2. Currently shows R1 – immediately before M2 – on PDF page 9 of 18

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

Current standards are sufficient and these changes are cosmetic. No changes to CIP-007 is required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

Mixed trust environment should not be permitted for BCS.

BCSI requirements are sufficient as in CIP-004 and CIP-011. Entities are compliant and appropriate controls are available to secure BCSI in current version.

Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based on security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

See MEC and BHE comments.

Likes 0	
Dislikes 0	

Response

Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6

Answer	No
Document Name	

Comment

Agree with SDT. If BCSI is not on the PCA, it should be identified as such because it would then not need to be protected. PCAs need to be included in to protect BCSI. Clarification in the guidance would be beneficial.

Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with the proposed changes to CIP-011 R2 part 2.1. The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for the basis of our response for this question.	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
For CIP-011-3 R2, the SDT consolidated former Parts 2.1 and 2.2 into a single requirement. Similar to R1, the applicability is expanded with conforming terminology that includes virtualization: “SCI hosting High or Medium Impact BCS or their associated: EACMS; PACS; or PCA.”	

Removal of Part 2.2 is a positive step that would allow Responsible Entities greater flexibility in dealing with sanitization of virtual systems. However, use of Cryptographic Erasure(CE) is complex and would require additional documentation for things such as key management and destruction records in order to demonstrate that the data is permanently irretrievable. In addition, all backup copies of the respective BCSI or BCS systems require destruction as well. This would need to be included in that standards to ensure that the entity has proper documentation to address the additional processes needed to address Cryptographic Erasure.

Likes 0

Dislikes 0

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0

Dislikes 0

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

NRG requests additional clarity with respect to scenarios where cryptographic erasure is allowed. This language is not referenced in either the Requirements or Measures sections of CIP-011 R2.1 but appears to be implied by virtue of the proposed changes. Thus, more explanation is needed.

Likes 0

Dislikes 0

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Comments: We agree with the combination of R2 part 2.1 and 2.2 as long as the language is further refined to address some CIP cyber assets such as PCA which may not contain BCSI at all.

Recommendations:

- We suggest retaining the language "contains BCSI" from the existing version, and consider the following wording for the new part 2.1:
    - "Method(s) to prevent the unauthorized retrieval of BCSI from applicable systems that contain BCSI prior to upon their disposal or reuse (except for reuse within other systems identified in the "Applicable Systems" column). "

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

NRG requests additional clarity with respect to scenarios where cryptographic erasure is allowed. This language is not referenced in either the Requirements or Measures sections of CIP-011 R2.1 but appears to be implied by virtue of the proposed changes. Thus, more explanation is needed.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: We agree with the combination of R2 part 2.1 and 2.2 as long as the language is further refined to address some CIP cyber assets such as PCA which may not contain BCSI at all.

Recommend:

- We suggest retaining the language "contains BCSI" from the existing version, and consider the following wording for the new part 2.1:

“Method(s) to prevent the unauthorized retrieval of BCSI from applicable systems that contain BCSI prior to upon their disposal or reuse (except for reuse within other systems identified in the “Applicable Systems” column). “

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Joshua Andersen - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

1. SRP is requesting a better description of what are the “allowing for cryptographic erasure in scenarios where BCSI cannot be mapped to particular disks within virtualized storage, and where BCSI is stored on SCI employing deduplication”. How would we perform an exercise for disposal an in Vitual world. Does cryptographic erasure need to be done on the virtual volume or in the physical storage?

2. SRP needs clarification on, “cryptographic erasure”. The term is not in the standard, only in the technical rationale. What does Virtual disposal look like? Please clarify what is necessary for evidence.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Consider revising to include a process to capture the encryption keys' management if using VMs/solid-state drives. The proposed language does not include the term "cryptographic erasure". Proposed language lacks the clarity to provide consistent application.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes made to R2, Subpart 2.1, however, EEI suggests that adding language, similar to what is used within the Technical Rationale, to the Measures column of Table R2 – Reuse and Disposal, bullet 1 to clarify that “cryptographic erasure in scenarios where BCSI cannot be mapped to a particular disk in virtualization storage” is an acceptable measure for this requirement.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 16.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	

Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the modifications to CIP-011 R2, Part 2.1. PG&E also supports the input provided by EEI for this modification.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE does not have comments on this question.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	

ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Tacoma Power noted the lack of Management Module inclusion in the Applicability column in CIP-011, and would like feedback from the SDT on whether this exclusion was intentional.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the proposed changes made to CIP-011 Requirement R2, Part 2.1.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with he proposed changes.	

Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
We support the NPCC TFIST and RSC comments and submit the following additional comments: Request correct label for R2. Currently shows R1 – immediately before M2 – on PDF page 9 of 18 Request review of the column Applicable Systems, Management modules and Management systems should be part of R1 and R2.	

Request clarification in the requirement to allow cryptographic erasure, this mecanism should not be in the requirement, the requirement should stay at the high level. Cryptographic merasure should me move to the Technical Rationale.	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC provides the following comments for the SDT's review and consideration: 9. In the proposed revisions for CIP-011, for applicable systems, it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., "…hosting [] impact BCS and the BCS's associated ….." or "….hosting [] impact BCS and the SCI's associated….." 10. In the applicable systems column, the reference to SCI includes an "or" and not an "and." This creates uncertainty as to whether both "their associated EACMS or PACS" must be managed or whether one or the other could be managed. This is different than what is used in current requirements and as related to BCS, which are "and" focused; thus, clarification and consistency in the listing of applicable systems is recommended to remove the potential for ambiguity and confusion. 11. A typographical error was identified in the form of duplicate R1s. It is suggested that the second R1 be revised to R2.	
Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
We can't say that we agree or disagree, it's not really clear what the intent is or what is being accomplished with the changes other than to add sci to the applicability column. Not sure I understand how the modification specifically allows for cryptographic erasure. We agree that management modules should be excluded from this requirement as that presumes that the module contains BCSI; this might be a stretch.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Request correct label for R2. Currently shows R1 – immediately before M2 – on PDF page 9 of 18	

Request review of the column Applicable Systems, Management modules and Management systems should be part of R1 and R2. Request clarification in the requirement to allow cryptographic erasure, this mecanism should not be in the requirement, the requirement should stay at the high level. Cryptographic merasure should me move to the Technical Rationale.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
We agree with the proposed changes to CIP-011 R2 part 2.1.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the proposed changes made to R2, Part 2.1, however, Southern requests that the SDT add language, similar to what is used within the Technical Rationale, to the Measures column of Table R2 – Reuse and Disposal, bullet 1 to clarify that “cryptographic erasure in scenarios where BCSI cannot be mapped to a particular disk in virtualization storage” is an acceptable measure for this requirement.	
Likes 0	
Dislikes 0	
Response	
Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Duke Energy generally agrees to the proposed modifications as the proposed language is flexible in allowing multiple methods.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	

Document Name	
Comment	
There is a typographical error on Page 9 where the requirement is labeled R1, but should say R2.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	
Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

17. The SDT performed a review of the CIP Standards and determined that CIP Exceptional Circumstances could be applied to the following additional requirements: CIP-004-7 Requirement R2 Part 2.2, CIP-004-7 Requirement R3 Part 3.5, CIP-006-7 Requirement R1 Part 1.8, CIP-006-7 Requirement R1 Part 1.9, CIP-006-7 Requirement R2, CIP-010-5 Requirement Part 1.2, and CIP-010-5 Requirement R1 Part 1.3. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Any place where CEC is added to the CIP requirements is desirable. It should be added to all CIP requirements, but it is understood that that is outside of this project's charter.

Likes 1	Jones Barry On Behalf of: sean erickson, Western Area Power Administration, 1, 6;
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: We do not find issue with applying exceptions to the existing standards, however implementing separate and diverse exceptions approach for certain requirements/parts or sub-requirements can cause issues for entities processes for declaring, establishing, managing and closing an Exceptional Circumstance. Recommend finding a method to consolidate an Exceptional Circumstance into a single process language.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Comments: We do not find issue with applying exceptions to the existing standards, however implementing separate and diverse exceptions approach for certain requirements/parts or sub-requirements can cause issues for entities processes for declaring, establishing, managing and closing an Exceptional Circumstance. Recommend finding a method to consolidate an Exceptional Circumstance into a single process language.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See Response to Question 1.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

We agree with the addition of CIP Exceptional Circumstances to the listed standards and requirements; however, we recommend adding CIP Exceptional Circumstance to CIP-006 Requirement R1 Parts 1.2 – 1.9.

Likes 0	
Dislikes 0	

Response

Erin Green - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Support the comments of Barry Jones (WAPA).	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We agree with the addition of CIP Exceptional Circumstances to the listed standards and requirements; however, we recommend adding CIP Exceptional Circumstance to CIP-006 Requirement R1 Parts 1.2 – 1.9.	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	No
Document Name	
Comment	
The parent requirement under CIP-006-7 R2 now includes “except during CIP Exceptional Circumstance” while the table seem to have removed “except during CIP Exceptional Circumstance” for Part 2.1. However, Part 2.2 has “except during CIP Exceptional Circumstance” included. The tables are used as our primary source of guidance and would be beneficial to have “except during CIP Exceptional Circumstance” in each of the applicable table(s).	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	

Comment	
Agree with the changes, but this should be part of a different SAR. These changes likely go beyond considerations for virtualization.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
Current standards are sufficient and these changes are cosmetic. No changes to CIP-007 are required to address Virtualization. Only applicability section needs to be modified along with BCS definition	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	No
Document Name	
Comment	

We do not find issue with applying exceptions to the existing standards, however implementing separate and diverse exceptions approach for certain requirements/parts or sub-requirements can cause issues for entities processes for declaring, establishing, managing, and closing an Exceptional Circumstance. Recommend finding a method to consolidate an Exceptional Circumstance into a single process language

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

We agree with the addition of CIP Exceptional Circumstances to the listed standards and requirements; however, we recommend adding CIP Exceptional Circumstance to CIP-006 Requirement R1 Parts 1.2 – 1.9.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

CPS Energy would recommend a method to consolidate CIP Exceptional Circumstance into a simplified process to include required documentation and perhaps CIP Senior Manager approval.

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1

Answer	No
Document Name	

Comment

Please see JEA coments, an individual response to my comment is not required.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
CIP Exception Circumstance already applies to CIP-004 Part 2.2. The SDT should consider adding CIP Exceptional Circumstance language to CIP-007 Part 4.1. Does the SDT intend for CIP Exceptional Circumstance language to apply to all of CIP-010 Part 1.2 or only Part 1.2.1? Does the SDT intend for CIP Exceptional Circumstance language to apply to all of CIP-010 Part 1.3 or only Part 1.3.1?	
Likes 0	
Dislikes 0	
Response	
Wayne Guttormson - SaskPower - 1	
Answer	No
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	Yes
Document Name	

Comment

{C}CIP-004-6 Requirement R2 Part 2.2 already includes CEC language. If the CEC language is already in CIP-006-7 Requirement R2 should it be removed from Part 2.2 as it was from Part 2.1?

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	Yes
Document Name	

Comment

Duke Energy agrees with the proposed modifications that CIP Exceptional Circumstances could be applied.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	Yes
Document Name	

Comment

Reclamation supports the inclusion of CIP Exceptional Circumstances where applicable.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Yes, Southern supports the addition of CEC language in each of these requirement parts.

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

No comments

Likes 0

Dislikes 0

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change

Likes 0

Dislikes 0

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes

Document Name	
Comment	
AZPS agrees with he proposed changes.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports these changes.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments, please see below: ACES agree with the SDT's changes to the above requirements, but if the SDT is adding CIP Exceptional Circumstances to various requirements, CIP-013 should also have an allowance for CIP Exceptional Circumstances for emergency procurements.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes

Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Texas RE proposes expanding the CIP Exceptional Circumstances exception to apply to all requirements. CIP Exceptional Circumstances can cover a variety of scenarios, may come at unexpected times, and may have unanticipated effects on a Registered Entity's ability to comply.

Additionally, Texas RE recommends CIP-003 be revised to require Registered Entities to report to their Regional Entities when compliance obligations have not been met due to a CIP Exceptional Circumstance. Texas RE believes that an approach similar to the COVID-19 self-logs in which entities report issues associated with CIP Exceptional Circumstances to the ERO within a prescribed amount of time. While the ERO may review these CIP Exceptional Circumstance log submissions, the expectation is that such submissions will be resolved without further enforcement action.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

ACES agree with the SDT's changes to the above requirements, but if the SDT is adding CIP Exceptional Circumstances to various requirements, CIP-013 should also have an allowance for CIP Exceptional Circumstances for emergency procurements.

Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3

Answer	Yes
Document Name	

Comment

Portland General Electric Company supports this change.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports these modifications.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 17.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports these changes.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	

Answer	Yes
Document Name	
Comment	
The SRC supports proposed changes to existing standards.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	Yes
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	
Document Name	

Comment
Please see comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

18. Implementation Plan: The SDT proposes an Implementation Plan that makes the revised CIP Standards and definitions effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order. However, the implementation plan allows a Responsible Entity to elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. Do you agree with this proposal? If you think an alternate effective date is needed, please provide a detailed explanation of actions and time needed.

Wayne Guttormson - SaskPower - 1

Answer	No
Document Name	

Comment

Support the MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Aaron Staley - Orlando Utilities Commission - 1

Answer	No
Document Name	

Comment

Please see JEA coments, an individual response to my comment is not required.

Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	No
Document Name	

Comment

The proposed changes that impact the CIP standards require significant changes to entities compliance program and associated documentation. Perhaps a staggered implementation plan or implementation after the effective date.

Likes 0	

Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI is concerned that, given the expansive changes proposed to accommodate virtualization, many entities will need additional time to implement changes. There is also a need for additional time because of the change from an asset-based approach to a systems-based approach. For many entities, this will require significant training and process modifications, as well as significant changes to existing compliance and asset management tools. While we appreciate the efforts being made to minimize entity impacts, even with those efforts, the industry will be faced with significant challenges and some naturally unexpected hurdles to ensure companies are adequately prepared. For this reason, we do not support a 24-month Implementation Plan but instead recommend the implementation of these change occur in a phased approach similar to the implementation for CIP Version 5

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 18,

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Will the Implementation Plan be updated? Currently shows CIP-012-1 as part of this project. We understand this project is not updating CIP-012. That CIP-012's initial mandatory date has not changed.

How will entities notify their Region? This question comes from the section titled "Compliance Dates for Early Adoption of Revised CIP Standards and Definitions." This section says "In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the Revised CIP Standards and Definitions."

Can the Rules of Procedure be modified to allow phased implementation by the mandatory date?

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

Given the extensive impact of the proposed changes to accommodate virtualization, an implementation timeline cannot be determined until the draft standards are closer to final.

When considering an implementation timeframe, we request the SDT consider the burden the new applicable systems, definitions and technology implementations will have to our current CIPv5 programs. There will be significant administrative burden to adjust documentation to accommodate the changes, as well as to revise programs and processes for requirements that are not backward compatible.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Concerned about the requirement for the entity to notify the region when adopting early. This process would force the entity to do an action but not force the Regions to facilitate the action. It does not seem that the notification would impact the CMEP. Does the entity have to adopt all of the Standards at one time or can this be phased in? Would notification be required as each portion of a phased implementation is completed? Suggest deletion of the requirement to notify regions.

Likes 0	

Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
Will the Implementation Plan be updated? Currently shows CIP-012-1 as part of this project. We understand this project is not updating CIP-012. That CIP-012's initial mandatory date has not changed How will entities notify their Region? This question comes from the section titled "Compliance Dates for Early Adoption of Revised CIP Standards and Definitions." This section says "In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the Revised CIP Standards and Definitions."	

Can the Rules of Procedure be modified to allow phased implementation by the mandatory date?	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS believes the time would be spent on adhering to the new defnitions proposed and the program changes associated with them, and therefore would request a longer timeframe for the effective date. AZPS recommends 6 additional month totalling 30 months.	

Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MEC and BHE comments.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Oklahoma Gas and Electric supports the comments provided by EEI.	
Likes 0	
Dislikes 0	

Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
More clarity needs to surround the Glossary of Terms before these standards go into place.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	No
Document Name	
Comment	
BC Hydro SME team’s preliminary impact assessment of the required changes based on the current CIP Standards’ drafts estimates that more than 36 months would be needed to fully implement these changes. SDT is requested to consider this when formulating the effective date of implementation for entities.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Given the extensive impact of the proposed changes to accommodate virtualization, an implementation timeline cannot be determined until the draft standards are closer to final.	

When considering an implementation timeframe, we request the SDT consider the burden the new applicable systems, definitions and technology implementations will have to our current CIPv5 programs. There will be significant administrative burden to adjust documentation to accommodate the changes, as well as to revise programs and processes for requirements that are not backward compatible.	
Likes 0	
Dislikes 0	
Response	
Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question	
Likes 0	
Dislikes 0	
Response	
Erin Green - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
Support the comments of Barry Jones (WAPA).	

Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Given the extensive impact of the proposed changes to accommodate virtualization, an implementation timeline cannot be determined until the draft standards are closer to final. When considering an implementation timeframe, we request the SDT consider the burden the new applicable systems, definitions and technology implementations will have to our current CIPv5 programs. There will be significant administrative burden to adjust documentation to accommodate the changes, as well as to revise programs and processes for requirements that are not backward compatible.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See Response to Question 1.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

Comments: Due to the extent of the changes to entities' existing compliance programs and associated documentation we would request a staggered implementation plan or at least 1 audit cycle – 3 years. We do not see the backward compatibility which was communicated early in the project.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: Due to the extent of the changes to entities' existing compliance programs and associated documentation we would request a staggered implementation plan or at least 1 audit cycle – 3 years. We do not see the backward compatibility which was communicated early in the project.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

TVA does not consider 24 months a sufficient amount of time to implement given the issues identified.

Likes 0	
Dislikes 0	

Response

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy recommends an implementation plan of 48 months with early-adoption options. In particular, the changes to CIP-005 will need to be implemented in a deliberate manner that does not disrupt reliable BES operations. These changes potentially require entities to make significant changes to management network architecture. Entities cannot prudently make significant investment associated with these changes until after FERC approval is obtained, so a longer period after the approval date is necessary for this standard than would be required for changes where FERC's intent to approve is clearer.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

CAISO signs on in support of SRC.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization

Answer	Yes
Document Name	

Comment

The SRC supports the proposed 24-month Implementation Plan (as a minimum) and the added flexibility for entities to transition to the revised standards and definitions prior to the effective date should they choose to do so. This assumes the SDT addresses the concerns raised in response to Question #1 concerning backward compatibility. Left unaddressed, SRC is concerned that entities may be required to expend significant administrative effort, akin to the level required in transitioning from V3 to V5, to modify existing program documentation merely to maintain status quo; i.e. to continue to comply with CIP standards absent any changes to adopt virtualization.

Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
The changes proposed will have significant impact on existing CIP programs in order to implement changes to configuration management systems, documentation, and possibly architecture. 24 months is the minimum that should be allowed to accommodate these changes.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E appreciates the work the Project 2016-02 Standard Drafting Team has put into these modifications and supports the 24 month Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le	
Answer	Yes

Document Name

Comment

FMPA supports a 24 months implementation plan.

Likes 0

Dislikes 0

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer Yes

Document Name

Comment

AEPCO is signing on to ACES comments.

Likes 0

Dislikes 0

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer Yes

Document Name

Comment

LCRA recommends that the NERC Evidence Request Tool is released immediately following FERC Board of approval. This tool may aide in the implementation of these revised standards.

Likes 0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer Yes

Document Name

Comment

AEP supports the 24-month implementation plan.

Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
LCRA recommends that the NERC Evidence Request Tool is released immediately following FERC Board of approval. This tool may aide in the implementation of these revised standards.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
No comments	

Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Yes, Southern supports the proposed Implementation Plan. Given the backwards compatibility of the proposed revisions, Southern appreciated the SDT’s efforts to ensure entities can choose the ways and means that best suit their own internal implementation timelines when moving from existing physical architectures to a more virtualized CIP environment.	
Likes 0	
Dislikes 0	
Response	
Shannon Ferdinand - Capital Power Corporation - 5 - MRO,WECC,Texas RE,SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Janelle Marriott Gill - Tri-State G and T Association, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Trevor Tidwell - Trevor Tidwell - 1,3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dania Colon - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victoria Mordi - Entergy - 3,7,9 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6	
Answer	
Document Name	
Comment	

Please see comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	

Likes 0	
Dislikes 0	
Response	

19. Please provide any additional comments for the SDT to consider, if desired.

Masuncha Bussey - Duke Energy - 1,3,5,6 - MRO,Texas RE,SERC, Group Name Duke Energy

Answer	
Document Name	

Comment

In addition to the above comments, Duke Energy recommends the following:

The proposed applicability of CIP-005 R1 component parts to EACMS and PACS, and in particular Part 1.5, is a major expansion of scope reminiscent of the “spaghetti requirements” – although it is appropriate to apply these protections to SCI, applying them to virtual EACMS and PACS is excessive in comparison to existing EACMS and PACS requirements.

The revised standards introduces multiple anti-affinity requirements that will increase the number of physical hosts required in clusters to maintain cluster reliability and compliance. Duke Energy agrees that it is reasonable to separate Intermediate Systems given their specific risks and functions as the “bastion host,” but requiring additional “trust levels” that separate BCA, Management Systems, other EACMS like Logging solutions, etc. within the virtual environment will add significant cost and complexity without commensurate cybersecurity benefits. Separating IS from other systems should provide a adequate, cost-justified level of separation based on the security requirements applied to those other systems hosted on SCI.

The inclusion of SCI in the PACS Maintenance and Testing requirements (CIP-006 R3) does not appear to be necessary or make practical sense. This requirement is clearly aimed at maintaining the integrity of the Physical Security Perimeter. Including the local badge controller portion of the PACS is technically sound, but the inclusion of the PACS server in current requirments was already confusing and required clarity in the G&TB. Now, the addition of SCI further exacerbates the question of what it means to test the PACS. What should be performed on SCI to meet this requirement? Even tests of provisioning and deprovisioning access that can reasonably include the PACS application servers cannot be applied to the SCI portion of the Applicable Systems. We suggest that the SDT use this opportunity to clarify that the scope of this requirement is the PACS components themselves (i.e. local controllers, application software) and remove the broader systems from the requirements’ applicability. At minimum, the SDT must provide clarity in the requirement as to what portion of the testing would apply to SCI.

Overall, the SDT’s approach solves certain problems with Virtualization, but in doing so, creates discrepancies in how the standards are applied between traditional and newer technologies. The creation of additional “device types” while not resolving the overall inconsistency in treatment of devices (e.g. CIP-002 now addressing BCS and SCI but not EACMS and PACS, applying requirements to PACS hosted on SCI but not those hosted on Cyber Assets) may confuse entities and auditors. Duke Energy recommends that the SAR be adjusted as needed to ensure the revisions produce a coherent approach to compliance, or that the SDT confine their changes to be more consistent with the existing defined terminology.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	
Document Name	

Comment

TVA welcomes changes to the standards that support innovation and increase security and reliability. However, the standards and supporting definitions as proposed lack sufficient clarity for effective implementation.

TVA supports an approach that embraces innovative technologies that enhance security and reliability. The proposed changes are myopic in requiring differentiation in virtualization technologies supporting compute, network, and storage resources. These distinctions are becoming increasingly indistinguishable as virtualization technologies evolve. Modern standards should make no distinctions in the treatment thereof, so as not to preclude adoption of emergent technology.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	
Document Name	

Comment

Comments:

The proposed changes would impact nearly all CIP standards. Edits to Applicability, for example, exceeds 170 changes. We believe the existing standard requirements could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, reduce the impact to entities' programs, and provide greater clarity to auditors.

Categorization: A virtual hardware platform operating multiple hosts including CIP and non-CIP hosts can be categorized as a single CIP Cyber Asset using the highest high water mark or with the multiple classifications. This clarifies compliance controls as technologies advance and operating systems, applications and components whether disks, arrays, solid state or chipsets. Once the virtual hardware platform operating multiple hosts are protected as the highest water marked CIP Cyber Asset, the CIP and non-CIP hosts can operate on the same hardware platform unless they share the CPU and memory.

Security Controls: The current CIP requirements for physical security, electronic access (authorization, authentication and accounting), software patch management, antimalware, vulnerability management, monitoring and logging, hardening, change and configuration management and supply chain establish security controls which prevent hosts within a hardware platform (virtual) from unauthorized communication or access to each. OSI layer 2 controls prevent communications ingress/egress each other (non-routed) on the hardware platform and virtual switch backplane.

Communications ingress/egress between the hardware platform (virtual server) hosts and non-hardware platform occurs at the OSI layer 3 and 4 via a routed protocol and identified EAP using the current language. This perspective allows an entity to use virtual hardware platforms independent of hosts categorizations.

Entities may not prefer to consolidate all hosts because of heightened risk (i.e. it puts many “eggs” in one basket) to the entire platform and/or system functions.

Using existing language and minor changes can give entities the flexibility to use virtual technologies. Virtual environments should contain differing levels of security within them. All physical Cyber Assets associated with a virtual environment, and associated software, should be high watermarked to the most secure classification.

The impacts to entities with the proposed changes are broad and deep. We recommend the SDT look to using existing language and concepts to address virtualization.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	
Document Name	
Comment	

Comments:

The proposed changes would impact nearly all CIP standards. Edits to Applicability, for example, exceeds 170 changes. We believe the existing standard requirements could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, reduce the impact to entities' programs, and provide greater clarity to auditors.

Categorization: A virtual hardware platform operating multiple hosts including CIP and non-CIP hosts can be categorized as a single CIP Cyber Asset using the highest high water mark or with the multiple classifications. This clarifies compliance controls as technologies advance and operating systems, applications and components whether disks, arrays, solid state or chipsets. Once the virtual hardware platform operating multiple hosts are protected as the highest water marked CIP Cyber Asset, the CIP and non-CIP hosts can operate on the same hardware platform unless they share the CPU and memory.

Security Controls: The current CIP requirements for physical security, electronic access (authorization, authentication and accounting), software patch management, antimalware, vulnerability management, monitoring and logging, hardening, change and configuration management and supply chain establish security controls which prevent hosts within a hardware platform (virtual) from unauthorized communication or access to each. OSI layer 2 controls prevent communications ingress/egress each other (non-routed) on the hardware platform and virtual switch backplane.

Communications ingress/egress between the hardware platform (virtual server) hosts and non-hardware platform occurs at the OSI layer 3 and 4 via a routed protocol and identified EAP using the current language. This perspective allows an entity to use virtual hardware platforms independent of hosts categorizations.

Entities may not prefer to consolidate all hosts because of heightened risk (i.e. it puts many “eggs” in one basket) to the entire platform and/or system functions.

Using existing language and minor changes can give entities the flexibility to use virtual technologies. Virtual environments should contain differing levels of security within them. All physical Cyber Assets associated with a virtual environment, and associated software, should be high watermarked to the most secure classification.

The impacts to entities with the proposed changes are broad and deep. We recommend the SDT look to using existing language and concepts to address virtualization.

Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	
Document Name	
Comment	
Please define the term “System Hardening”.	
Likes 0	
Dislikes 0	
Response	
Cristhian Godoy - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	
Document Name	
Comment	
In our assessment, the risk of sharing infrastructure across different security zones (BES Cyber Systems vs. non-BES Cyber Systems) is higher than the benefit gained from such virtualization. Con Edison and Orange & Rockland Utilities fully concur on the benefits of virtualizing within same ‘level’ security zones, but entities should not be virtualizing across trusted to untrusted security zones. We do not believe it is appropriate for SCI to be share across BES Cyber Systems and non-BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
Reclamation recommends that improved resilience or reliability of the BES be the primary consideration before an entity adopts any new or emerging technologies for BES reliability operating services.	

Reclamation also recommends utilizing existing FedRAMP criteria and air gapping Industrial Control Systems where possible from external communications.

Remove language in the new definitions and in any Requirement that refers to a third person (their).

Reclamation understands the driver for this round of comments, and requests that the SDT submit smaller packets of data for future rounds of commenting and balloting. This was a heavy lift for a resource-constrained entity to review with the depth and seriousness warranted.

Reclamation appreciates SDT efforts to incorporate NIST Framework into the NERC Standards and encourages the SDT to continue this practice moving forward by ensuring that requirements are not duplicated within the NERC Standards where they may overlap NIST Framework.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	
Document Name	

Comment

ISO-NE believes that the SDT's approach solves certain problems with virtualization. However, as mentioned in earlier comments, it also creates increased complexity and discrepancies in how the definitions and requirements are applied. Because of the new definitions, there is a mixing/matching of virtual and physical systems. The creation of additional "device types" while not resolving the overall inconsistency in treatment of devices may confuse both Registered Entities and auditors. ISO-NE recommends that the SDT consider the suggestions presented in the comments above, as well as carefully review and adjust the "Applicable Systems" column for consistency and to limit confusion across all CIP Standards.

Furthermore, ISO-NE recommends the added language in CIP-010 R3.2, "...that minimizes difference with the production environment…" be deleted because CIP-010 Part 3.3.2 requires that the differences between the test environment and production environment be documented.

ISO-NE appreciates the opportunity to comment.

Likes 0

Dislikes 0

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer

Document Name

Comment

NRG requests that the Guidelines and Technical Basis sections be added back in instances where they were removed. Furthermore, NRG believes that examples in the Guideline and Technical Basis would prove helpful in instances where significant changes were made (i.e. diagrams depicting logical isolation for SCI, examples of management modules, etc.).

Likes 0

Dislikes 0

Response

Marty Hostler - Northern California Power Agency - 5

Answer

Document Name

Comment

See Response to Question 1.

Likes 0

Dislikes 0

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer

Document Name

Comment

Under CIP-005-8 R1.5, Southern requests the SDT consider the following changes to the proposed edits to specify IP “network” communications:

Detect known or suspected malicious Internet Protocol (IP) ***network*** *communications for both inbound and outbound* ***network*** *communications entering or leaving the logical isolation required by Part 1.1 or Part 1.2.2.*

Additionally, under CIP-005-8 R1.5, the proposed revisions to remove EAPs associated with high BCS and mediums at Control Centers and add PACS and EACMS hosted on SCI significantly increases the scope and adds requirements previously not applicable to those Applicable Systems. As with our previous comment, the use of the conjunctions “and” and “or” when referring to “and their associated:” is not used here consistently; this further supports our comments that applying these new requirements to PACS and EACMS should only apply when those systems are “hosted on the same SCI as a h/m BCS”, and are not justified from a risk-based perspective when simply considering stand-alone virtual PACS or EACMS that are not hosted on the same SCI as a h/m BCS.

Although there was no question related to conforming changes for CIP-013-3, Southern supports the conforming change edits to CIP-013-3 given that the SDT is able to adequately address our other comments contained herein.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	
Document Name	

Comment

Management Systems for non-virtual environments should be protected at the same level as the Management Systems for SCI; we understand that the SAR limited the SDT. Likely this could be captured by FERC as a conditional approval item for the next version of CIP Standards.

Please keep ESP and EAP as NERC Glossary terms. This may avoid future auditor interpretation issues and allow consistent application of the concepts across industry. It also helps preserve backward compatibility.

Please provide a draft copy of the NERC CIP ERT for the new requirements with the next posting. This would help entities assess the impacts the proposed changes would have to managing audit preparation under the new requirements.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	
Document Name	

Comment

N/A

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer

Document Name

Comment

No other comments

Likes 0

Dislikes 0

Response

Andrea Barclay - Georgia System Operations Corporation - 4

Answer

Document Name

Comment

GSOC respectfully provides the following general comments:

1. Relative to VSLs, the proposed revisions inconsistently refer to the assets more explicitly, e.g., BCS, SCI, etc., in some instances while utilizing Applicable Systems in other instances. Consistency is recommended in the drafting and development of VSLs. Further, to reduce the potential for error, it is recommended that the term “applicable systems” be utilized whenever possible.

2. Relative to titles and purpose, GSOC noted several titles and purpose with proposed revisions as well as those that did not have proposed revisions despite revisions that broadened their overall scope and applicability. To ensure consistency amongst the reliability standards and with the broader scope of applicable systems, GSOC recommends that these be evaluated holistically to identify the need for any additional conforming revisions.

3. Generally, the formatting of applicable systems within the applicable systems column should be evaluated for consistency of format.

4. In the proposed revisions, for applicable systems, it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on

these along with attendant revisions for clarity are requested, e.g., “…hosting [] impact BCS and the BCS’s associated …..” or “….hosting [] impact BCS and the SCI’s associated…..”

5. In the applicable systems column, scoping of applicable systems with additional terms such as ERC, IRA, etc. seems to be inconsistently applied. While it is understood that these scope additions better tailor the requirements, inconsistent application and use of scoping verbiage can lead to ambiguity and confusion. For this reason, review of these scope additions and use of consistent scoping of verbiage is recommended.

6. Relative to CIP-013, which had conforming revisions only, GSOC provides the following comments for the SDT’s review and consideration:

a. In the proposed revisions for CIP-013, , it is unclear whether the addition of SCI and attendant bullets results in the inclusion of the EACMS and PACS associated with the SCI or whether it is the EACMS and PACS associated with the BCS that is being hosted by the SCI. Clarification on these along with attendant revisions for clarity are requested, e.g., “…hosting [] impact BCS and the BCS’s associated …..” or “….hosting [] impact BCS and the SCI’s associated…..”

b. The verbiage utilized in the VSLs differs from the verbiage utilized in the requirements and raises a questions as to whether the EACMS and PACS of SCI are in scope for the standard.

c. A typographical error was identified in requirement R1. Controlling should be revised to Control.

Likes 1	Georgia Transmission Corporation, 1, Davis Greg
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

Management Systems for non-virtual environments should be protected at the same level as the Management Systems for SCI; we understand that the SAR limited the SDT. Likely this could be captured by FERC as a conditional approval item for the next version of CIP Standards.

Please keep ESP and EAP as NERC Glossary terms. This may avoid future auditor interpretation issues and allow consistent application of the concepts across industry. It also helps preserve backward compatibility.

Please provide a draft copy of the NERC CIP ERT for the new requirements with the next posting. This would help entities assess the impacts the proposed changes would have to managing audit preparationunder the new requirements.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for details.

Likes 0	

Dislikes 0

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer

Document Name

Comment

The CPU and memory isolation language in the PCA definition, CIP-005 R1.2, and CIP-005 R2.6 are a poison pill to this draft. They create a 4-tier structure to virtualization; BCAs/PCAs, Management Systems, Intermediate Systems, and all other VMs. On a non-CIP system, such VMs could be hosted on a 4-node cluster and have suitable redundancy. Under the draft standards, none of these classifications can share CPU or memory with any other classification. This represents a potential doubling and possibly more of the infrastructure required, as you would need to have at least 2 hosts for BCA/PCA, 2 hosts for Management Systems, 2 hosts for Intermediate systems, and 2 hosts for other systems (for total of at least 8, with the potential for more given TOP-001 redundancy requirements), along with vastly increased complexity to prevent VMs of different classifications from running on the same host.

This added complexity introduces risk, where a failure could render BCA unable to find an appropriate host to run, even when plenty of resources are available. All this cost and complexity is added to mitigate vulnerabilities that do not exist yet and are only theoretical (that is, a side channel remote execution or privilege escalation that crosses VM boundaries). The cited side channel attack by the SDT (row hammer) has not been seen in the wild and has not been shown to allow VM escape.

Possibly one of these isolation requirements would be acceptable, but 3 separete ones make this untenable.

Furthermore, these threats are already covered by two other CIP requirements. In the event that such vulnerabilities were discovered, either patches would be released that could be applied as required by CIP-007 R2 (or if the patches cannot be installed, a mitigation employed), or an entity would identify the vulnerability in their CIP-010 R3 vulnerability assessment and mitigate them as part of their action plan. With these proposed requirements, the SDT cripples the ability for entities to implement virtualization at all, essentially cutting off one’s hand to prevent getting a splinter.

These CPU/memory isolation requirements place virtualization out of the reach of smaller entities and greatly eliminate the benefits for even larger entities. Approval of this draft would require entities who have already implemented virtualization to completely rearchitect their systems, or potentially scrap their virtual infrastructure all together due to the added burden. It also mandates a specific control to address a concern (isolate VMs), rather than addressing the underlying need (mitigate side-channel vulnerabilities), which is counter to the SDT’s stated goal of not requiring the “how” but requiring the “what”. If the SDT wishes to address side-channel vulnerabilities, it should do so in a separate SAR that looks at how entities address vulnerabilities (similar to a previous draft that combined CIP-007 R2 and CIP-010 R3). We believe these changes introduce a poison pill to the new draft which significantly increases the likelihood of rejection by industry.

Likes 0

Dislikes 0

Response

Victoria Mordi - Entergy - 3,7,9 - SERC

Answer

Document Name

Comment	
Entergy is concerned by the wholesale deletion of the Guidelines & Technical Basis section of each standard addressed by this revision. These sections provided valuable guidance and information used to develop and document compliance positions or interpretations. The loss of this information would increase ambiguity with the standards and potentially call into question long standing compliance interpretations. Entergy does not support the deletion of this information.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1	
Answer	
Document Name	
Comment	
Similar to CIP-005-8, CIP-007-7 and CIP-010-5 Draft 1 versions, BC Hydro recommends that a reference to the Technical Rationale documents be included within the Associated Documents section of the Standard.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	
Document Name	
Comment	
Suggest not to include PACS and EACMS in the scope in the context of SCI as this requirement doesn't exist for a PACS and EACMS not on a SCI. SAR is for including the virilization concepts not to add additional controls. Suggest reviewing the Applicable Systems of the different CIP associated to management modules. The current langage only refers to a Management Modules of SCI hosting. What about a the management module of a BCA ? Management Modules of SCI hosting would have more controls than a Management Modules of BCA. The SDT should look into the CMEP Practice Guides published on the NERC web site. The following documents; CMEP Practice Guide Virtual Systems, CMEP Practice Guide Virtual Network, CMEP Practice Guide Virtual Storage are pertaining to the virtualization and they contain enough elements for us to understand what needs to be done to be compliant. Those CMEP documents permit the usage of the virtualization with the current concepts and definitions. The SDT should use those documents and update the different CIPs documents with the required and corresponding wording.	

Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	
Where technically feasible' -> 'Per system capability' **MRO Comment:** There are instances of 'per system capability' replacing 'where technically feasible' that could allow for fewer protections for those BCS. TFEs required "Compensating and mitigating measures" (NERC ROP Appendix 4D). This is no longer required and limits compliance monitoring. (Consider an EACMS or PACS, which do not require logical isolation, not requiring authentication [Part 5.1] or limiting authentication attempts [Part 5.7]. This poses an increased risk.) **Recommendation:** Modify the language of the requirements beyond just replacing 'where technical feasible' with 'per system capability' to better address risk posed by the lack of the required controls.	
Likes 0	
Dislikes 0	
Response	
Colleen Peterson - Basin Electric Power Cooperative - 1,3,5,6	
Answer	
Document Name	
Comment	
Please consider how these virtualization standards apply to the cloud. The SDT stated that this is not intended for cloud implement; is this defined in the standards? These changes could contradict or be overly restrictive based on previous NERC guidance on BCSI in the cloud.	
Likes 0	
Dislikes 0	
Response	
Joshua Andersen - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	Project 2016 Q19 response.docx

Comment

See the attached file.

Likes 0

Dislikes 0

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer

Document Name

Comment

See MEC and BHE comments.

Likes 0

Dislikes 0

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer

Document Name

Comment

It seems as though there are some inconcistencies within the applicable systems column throughout the standards. Is that the intent of the SDT? For instance, the applicable systems column in CIP-005 R1.1 contains PCAs and PACs and EACMS hosted on SCI. However, thoughout most of the other standards, the requirements list SCI hosting High or Medium Impact BCS with the associate PACS, PCS, and EACMS. There are several things that are not completely clear in this approach. It is unclear what the purpose of the phrase “hosted on SCI” is associated with PACS and EACMS. Would the requirement not apply if the PACS or EACMS is hosted on SCI or not in the CIP-005 R1.1? Based on the requirement language, it seems as though it shouldn’t matter whether they are hosted on SCI or not. Further clarification is needed around the intent of either the phrase “hosted on SCI” or what the intent of requirement is. Additionally, when the phrasing is used that includes that language “SCI with ERC hosting High and Medium Impact BCS or their associated PACS, EACMS, or PCA,” is the intent that only the BCS must be hosted on the SCI and the associated systems do not need to be hosted on SCI? An example of this language can be found in CIP-007 R4.1.

Likes 0

Dislikes 0

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	
Document Name	
Comment	
MPC supports comments submitted by Duke Energy.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	

Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	
Document Name	
Comment	
Need clarification on CIP-005 R1.2.1 - Why restrict management systems to only share CPU with other Management Systems? Would it not be better to say BCS can only share CPU with other BCS? Can CPU be shared across Management Systems for BCAs and Management Systems for Non-BES Cyber Assets? Would you be able to clarify virtual CPU vs. physical CPU separation?	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	
LCRA views many of these revisions as administrative in nature. They will require additional resources to update and reformat a NERC CIP Program. The result is a change to how programs are documented but not to security. Additionally, the rapid revisions of CIP Standards result in entities having to continually tweak their internal processes for collecting evidence and to ensure consistency with new terminology. Again, this is a concern if security is not being enhanced.	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6

Answer	
Document Name	

Comment

AEP appreciates the work of the SDT in addressing potential gaps related to virtualization in the currently enforceable language of the CIP Standards. It has been AEP's experience that there is adequate flexibility in the application of the current CIP Standards/requirements to allow for the implementation of Virtualization both as BES Cyber Assets/Systems, as well as the associated EACMS, PACS and/or PCA. This experience is based in Regional Entity(ies) audit of the virtualized environments that are currently operating in production CIP environments. We would further point out that the security and auditability of these systems, within the framework of the existing Standards, is supported by the CMEP Practice Guides released by NERC on 3/1/2021 (on the subjects of Virtual Network, Virtual Storage, and Virtual Systems).

Given prior successful audit of virtualized Assets within AEP's CIP environments, AEP recommends to consider limiting the introduction of new terms/definition to only those areas where it is necessary to reach an end result of increased security, resiliency and/or sustainability. AEP does, however, commend the movement away from heavily burdensome time-based requirements in favor of security-driven and objective-based requirements.

Please Note: one of AEP's balloters accidentally selected "Negative Opinion" for the CIP-002-7 Non-binding Poll. The intent was to select "No Opinion". While unable to change a vote once cast, AEP felt it was important to inform the SDT of the true intent of the vote.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	
Document Name	

Comment

LCRA views many of these revisions as administrative in nature. They will require additional resources to update and reformat a NERC CIP Program. The result is a change to how programs are documented but not to security.

Additionally, the rapid revisions of CIP Standards result in entities having to continually tweak their internal processes for collecting evidence and to ensure consistency with new terminology. Again, this is a concern if security is not being enhanced.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
We would like to thank the SDT for their hard work and would like to thank the SDT for allowing us to comment on the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	
Comment	
We continue to encourage the Standard Drafting Team to maintain full backward compatibility.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	
Document Name	

Comment

CIP-006, R2 added “except during CIP Exceptional Circumstances” to the root requirement, but removed it from part 2.1. Are we to assume that the root requirement allowing CIP Exceptional Circumstances would flow down to the sub-parts? If so, why was If not removed from 2.2? If not, does this mean that first responders would be required to escorted? Clarity to the intent of the applicablility of this phrase would be appreciated.

The definition of IRA still leaves some room for interpretation. While DOminion Energy supports simpolifying the definition, the IRA definition should address the communication session that ends with the destination asset. The session between the asset (physical or virtual Cyber Asset) and the Intermediate System is user initiated. The session between the Intermediate System and the destination asset is user initiated.

A management console, for this example, does not have constant communication sessions with client Cyber Assets/Virtual Cyber Assets unless the console needs to execute a command on a client. A user establishes a session with the console, via multi-factor authentication, and instructs the console to execute a command on a client. In order to execute the command, the console needs to establish a communication session with the client.

Is a connection from console to a Cyber Asset client also a user-initiated IRA if the user schedules on the console a configuration command that will execute one hour later by the console (and after the user had ended the communication session to the console)? What if the user schedules a command for execution by the console within 5 minutes? Is this user-initiated IRA too? Would the console itself be an Intermediate System? The current language is ambiguos on these issues.

In both scenarios, the console establishes the communication sessions to the client asset and the sessions are not between the user and the client. Rather than leave the interpretation to the Entities or Regional Entities, the IRA definition should have more clarity built-in to address such scenarios.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	
Document Name	

Comment

Generic Formatting Comments

Issue 1:

The “Management Module” inclusion across the Standards is inconsistent with the inclusion of “Shared Cyber Infrastructure.” Tacoma Power believes there are additional locations where the risk posed by Management Modules is equivalent to the risk posed by the SCI itself and these should also include Management Modules as applicable. Tacoma Power suggests that there may be a way within the Applicability Section of the Standard to state that where SCI is included in the applicability of a requirement, any associated Management Modules are also included. This would avoid the issue of including one cyber asset within another, and the hall of mirrors that builds, which would happen if the SDT were to simply ensure Management Modules were included in the SCI definition. It would also simplify the Applicability Columns throughout. Another possible solution would be notating each SCI applicability inclusion with a footnote, then including the statement that each inclusion of SCI also includes any associated Management Modules, as a footnote on each applicable page.

Issue 2:

Review each Standard’s Applicability column to ensure the sub-bullet formatting and order of the “associated” PACS, EACMS, and PCA is consistent from unaltered to newly inserted items and across all Standards.

Issue 3:

The SDT should consider stating “per system or component capability” in the Requirement language instead of “per system capability”. Requirements are applied at either the system or component level. Because there is inconsistency with the “level” of a Requirement’s object across the CIP Standards, this change may add some necessary clarity.

CIP-005 General Comments

Issue 1:

Tacoma Power seeks clarification from the SDT on the directional language used in CIP-005. For example, the Standard uses “to and from”, “leaving and entering”, and “between”. This inconsistency could be confusing depending on the context, consistency of usage could add clarity throughout the Standard.

Issue 2:

Comment on CIP-005 Technical Rationale, “Shared infrastructure and ‘Mixed Trust’ Risks”: While Tacoma Power is not voting against this rationale document, we feel that affinity is not an adequate control to ensure SCI security in a mixed trust environment, because affinity controls exist on individual servers to split processor core access or RAM NUMA Node access.

In line with the above statement, perhaps changing the terminology used in describing the Affinity rule requirements (CIP-005 R1 Part 1.2, and CIP-005 R2 Part 2.6) to “Host or Cluster Affinity and Anti-Affinity rules” would provide more clarity to industry. Host Affinity is a VMWare Term, while Cluster Affinity is a Hyper-V term.

CIP-007 General Comments

Issue 1:

CIP-007 R1 Part 1.2 applicability column “Management Modules” entry includes PACS and EACMS where the rest of the Applicability entries do not, is this intentional? This appears to be a mistake.

Issue 2:

In CIP-007 R5 Part 5.7, the SCI entry in the Applicable Systems column includes “with ERC” which should be removed, as follows: “SCI at Control Centers hosting High Impact BCS, Medium Impact BCS or their associated:” Alternatively, Tacoma Power recommends the SDT re-word this applicability to state: “SCI hosting High Impact or Medium Impact at Control Centers or their associated:”

Issue 3:

While it may not be part of the SAR scope for Project 2016-02, Tacoma Power recommends that the SDT consider removing “at Control Centers” from the Applicability Statements from CIP-007 R5 Part 5.7 to enforce this control on those remote elements that are typically more exposed to attack.

CIP-010 General Comments

Issue 1:

The CIP-010 R2 Applicable Systems column omits SCI and Management Modules. Tacoma Power would like feedback from the SDT on whether this exclusion was intentional.

Issue 2:

Tacoma Power recommends that the SDT review and revise CIP-010, Attachment 1 to include SCI. There are instances of “BES Cyber System” which do not have the typical SCI redlined in.

Consistency with Project 2017-07

Project 2017-07 stated that “CIP-002-5.1a, CIP-003-6, CIP-003-7, CIP-004-6, CIP-005-5, CIP-005-6, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, and CIP-011-2 will not be revised at this time due to the current Project 2016-02 (Modifications to CIP Standards) and the CIP Standards Efficiency Review.” The currently posted redlines for Project 2016-02 do not include all of the Standards Alignment changes (e.g. “UFLS-only DP”). Tacoma Power recommends the SDT document whether this project or the CIP Standards Efficiency Review will closeout these updates.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	
Document Name	

Comment

Ameren agrees with and supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 1,3,5,6

Answer	
Document Name	

Comment

Please see comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

Please see comments submitted by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Dania Colon - Orlando Utilities Commission - 5

Answer	
Document Name	

Comment

Too much compartmentalization based on non-industry standard definition. Please review NIST Publication 800-125 (virtualization guidelines) and apply controls, based on Terms such as Management Systems, Guest, Hosts, Network virtualization, Infrastructure virtualization (Mixed Trust, Resources sharing, high-watermarking) and similar guidance that is used by Industry, SME and vendors. SDT approach is complicated and confusing which will result in different interpretation by SMEs and ERO.

SDT draft utilizes non-industry standards requirements and terminology, and will result in confusion and subjective and varying application. Recommend that SDT use Industry standard terminology such as NIST or PCI-DSS and security controls as laid out in such frameworks.

All definitions should be contextualized in relation to BES application.

Furthermore, require standard requirements to apply control application based on risk to the systems based industry standard approaches such as high watermarking practices instead of compartmentalizing security controls based on every unique device types that SDT has identified.

SDT has summarily discarded Industry standard practices such as baselining but replaces it with subjective terms such as hardening, which varies depending on environment and device types. Such scenario will lead to different conclusions by the auditors and entity SME.

It has taken four years for the industry to standardize the security and baselining requirement. New approach discards all the work done so far and creates confusing set of expectations.

Further, in CIP-010, tracking hardening requirements in change management tickets is an incorrect approach as CM is for tracking activities and not performing assessments and compare of configurations.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	
Document Name	

Comment

Request clarification on CIP-005 R1.4 “per system capability.” Who determines that capability? What evidence do the auditors expect?

Request clarification on CIP-005 R2.3 “Multi-Factor Authentication (MFA).” Years ago, two step verification (2SV) was generally accepted as MFA. 2SV uses SMS which is hackable. Does this MFA expectation include 2SV?

Request consistency between CIP-005 R2.4 and R2.5. R2.5 Requirement uses abbreviation (IRA). R2.4 does not.

Several comments on CIP-005 R2.6; 1) the Applicable System should be explicitly stated; 2) we are concerned with how complex (difficult) Applicable Systems and Definitions are to comprehend; 3) is an Intermediate System *only* an Intermediate System; 4) does R2.6.2 allow communications with a remote system? 5) if Intermediate System is used only in R2, it should not be a defined term. The explanation and use of Intermediate System should be in only R2

Three comments on CIP-010 R3.2. These comments were repeated for CIP-010 R1.3. 1) request removal of “minimizes differences with the production environment” because new language is a) subjective, b) better suited to the measures and c) the previous language is sufficient 2) if this language cannot be removed, request clarification that the entity determines “minimal differences” 3) suggest that the intent is to a) test and b) document what was tested

For CIP-010 R3, request that the SCI requirement into a separate Part. Same comment was made for CIP-010 R1

One comment on CIP-007 R1.3. Request consistent language on the exclusion of services that cannot be disabled. Consistent with R1.1.

One comment on CIP-007 R2. Concerned about this language. The proposed language is “systems.” However, patches are applied to assets. This concern is repeated in CIP-007 R4.1, R4.2, R4.3, R5.4, R5.5, R5.6

One comment on CIP-007 R3.1 Measures. This is a repeat of a general comment on CIP-007. The use of “system hardening” here seems different than “system hardening” elsewhere in CIP-007. Request consistent use of this label. How does one measure “system hardening.” What evidence will the auditors expect?

Likes 0

Dislikes 0

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer

Document Name

Comment

ITC supports the response/comments submitted by EEI

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

This is a significant change and overhaul of all the CIP Standards and Requirements that will require a significant re-analysis of stable and current CIP Standards and Requirements and definitions. Today, virtualization is used with the understanding that the VM host receives the “high water mark” of the VMs hosted, which is a simplified approach that doesn’t require new definitions. Texas RE cautions the splitting of compliance and security controls to components of VM host(s) in virtualization.

Likes 0

Dislikes 0

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer

Document Name

Comment

N/A.

Likes 0

Dislikes 0

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer

Document Name

Comment

Wabash Valley appreciates the effort that the Standards Development Team has put into development of this standard. However, significant additional work and documented guidance such as those that would previously have been found in the Guidelines and Technical Basis Section of the CIP Standards is needed and should be a mandatory consideration of CMEP teams. The removal of these sections has been a detriment to the CIP Reliability Standards.

Likes 0

Dislikes 0

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer

Document Name

Comment

We would like to thank the SDT for their hard work and would like to thank the SDT for allowing us to comment on the proposed changes.

Likes 0

Dislikes 0

Response

Truong Le - Truong Le On Behalf of: Neville Bowen, Ocala Utility Services, 3; - Truong Le

Answer

Document Name

Comment

N/A

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	
Document Name	

Comment

no further, thank you.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	
Document Name	

Comment

For CIP-006 R2.2 – Request removal of “except during CIP Exceptional Circumstances” from R2.2. See the requirement column. This language was moved to R2. So, this exception already applies to this Part.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	
Document Name	

Comment

SPP wants to the thank the SDT for their work on this complex project and understands the time and effort that goes into an undertaking such as this.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 1, 3, 5; Marco Rios, Pacific Gas and Electric Company, 1, 3, 5; Sandra Ellis, Pacific Gas and Electric Company, 1, 3, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	
Document Name	

Comment

PG&E has no further comments related to this Command & Ballot.

Likes 0	
Dislikes 0	

Response

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	
Document Name	

Comment

Management Systems for non-virtual environments should be protected at the same level as the Management Systems for SCI; we understand that the SAR limited the SDT. Likely this could be captured by FERC as a conditional approval item for the next version of CIP Standards.

Please keep ESP and EAP as NERC Glossary terms. This may avoid future auditor interpretation issues and allow consistent application of the concepts across industry. It also helps preserve backward compatibility.

Please provide a draft copy of the NERC CIP ERT for the new requirements with the next posting. This would help entities assess the impacts the proposed changes would have to managing audit preparationunder the new requirements.

The exemption language in section 4.2 of every CIP standard needs to be addressed, please see our response for Question 9 for details.

Likes 0	
Dislikes 0	

Response

Jose Avendano Mora - Edison International - Southern California Edison Company - 1,3,5,6

Answer	

Document Name

Comment

Please see comments submitted by the Edison Electric Institute

Likes 0

Dislikes 0

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer

Document Name

Comment

PJM signs on to the comments provided by the SRC and submits the following additional comments:

1) PJM requests additional clarity surrounding the removal of the term “or” in CIP-007 R2.3. Does this change the context of the standard or was the second “or” kept intentionally to provide choice in the list of actions? Recommendation: remove the second “or” for consistency.

2) PJM identifies that the CIP 011 requirements are being modified to focus on the BCSI itself and not the actual Cyber Assets identified in the “Applicable Systems” column. PJM recommends that the applicable systems column should include "BCSI repositories" rather than the Cyber Assets identified in the “Applicable Systems” column, given that the requirements are being modified to focus on the BCSI itself and not the Cyber Assets.

3) PJM also requests SDT to confirm intention of listing SCI with EACMS, PACS, and PCA in the applicable system sections which seems repetitive. The new definitions for EACMS, PACs, and PCAs now includes SCI which makes the Applicable Systems section repetitive when listing “SCI hosting High or medium impact BCS or their associated EACMS, PACS, and PCA”.

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer

Document Name

Comment

Request clarification on CIP-005 R1.4 “per system capability.” Who determines that capability? What evidence do the auditors expect?

Request clarification on CIP-005 R1.5. The proposed language does not include the combination of non-IP and malicious. Is this acceptable?

Request clarification on CIP-005 R2.3 “Multi-Factor Authentication (MFA).” Years ago, two-step verification (2SV) was generally accepted as MFA. 2SV uses SMS which is hackable. Does this MFA expectation include 2SV?

Suggest a CIP Standard should not explicitly reference a Standard not in NERC’s purview in Requirement language. If the inclusion is necessary, request correction of CIP-005 R2.4’s references to GOOSE protocol - “IEC TR-61850-90-5 R_GOOSE.” We believe SDT should reference 1) IEC/TR 61850-90-5:2012 / Part 90-5: Use of IEC 61850 to transmit Synchrophasor information according to IEEE C37.118 and 2) IEC 61850-8-1 GOOSE (Generic Object-Oriented Substation Event message) and IEC 61850-9-2 SV packets. CIP-003 may have shared this concern.

Request consistency between CIP-005 R2.4 and R2.5. R2.5 Requirement uses abbreviation (IRA). R2.4 does not.

Several comments on CIP-005 R2.6; 1) the Applicable System should be explicitly stated; 2) we are concerned with how complex (difficult) Applicable Systems and Definitions are to comprehend; 3) is an Intermediate System *only* an Intermediate System; 4) does R2.6.2 allow communications with a remote system? 5) if Intermediate System is used only in R2, should not be a defined term. The explanation and use of the Intermediate System should be in only R2

Two comments on CIP-005 R3. 1) system to system communications is not currently defined. Is system to system included in R3? The issue is that that “system to system” is nebulous; 2) request an illustration/diagram since this is hard to follow

Three comments on CIP-010 R3.2. These comments were repeated for CIP-010 R1.3. 1) request removal of “minimizes differences with the production environment” because new language is a) subjective, b) better suited to the measures and c) the previous language is sufficient 2) if this language cannot be removed, request clarification that the entity determines “minimal differences” 3) suggest that the intent is to a) test and b) document what was tested

For CIP-010 R3, request that the SCI requirement into a separate Part. The same comment was made for CIP-010 R1

One comment on CIP-007 R1.3. Request “consistent” language on the exclusion of services that cannot be disabled. Consistent with R1.1.

One comment on CIP-007 R2. Concerned about this language. The proposed language is “systems.” However, patches are applied to assets. This concern is repeated in CIP-007 R4.1, R4.2, R4.3, R5.4, R5.5, R5.6

One comment on CIP-007 R3.1 Measures. This is a repeat of a general comment on CIP-007. The use of “system hardening” here seems different than “system hardening” elsewhere in CIP-007. Request consistent use of this label. How does one measure “system hardening?” What evidence will the auditors expect?

Suggest not to include PACS and EACMS into the scope in the context of SCI as this requirement doesn’t exist for a PACS and EACMS, not on an SCI. SAR is for including the virilization concepts not to add additional controls.

Suggest reviewing the Applicable Systems of the different CIP associated with management modules. The current language only refers to Management Modules of SCI hosting what about the management module of a BCA? Management Modules of SCI hosting would have more controls than Management Modules of BCA.

SDT should look into the CMEP Practice Guides publish on the NERC website. The following documents; CMEP Practice Guide Virtual Systems, CMEP Practice Guide Virtual Network, CMEP Practice Guide Virtual Storage is pertaining to virtualization and they contain enough elements for us to understand what needs to be done to be compliant. Those CMEP documents permit the usage of virtualization with the current concepts and definitions. SDT should use those documents and update the different CIPs documents with the required and corresponding wording.

Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Douglas Webb	
Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference Edison Electric Institutes (EEI) response to Question 19,	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
Every CIP Reliability Standard currently in effect makes every Distribution Provider that owns underfrequency (UFLS) systems that meets the subparts identified in 4.1.2.1.1 and 4.1.2.1.2 applicable to the CIP Standards, however, UFLS only Distribution Providers that may also meet these criteria are not currently applicable to any of these standards. EEI requests that this gap be addressed by adding UFLS only Distribution Provides that meet the identified criteria to be made applicable to these Reliability Standards. EEI seeks clarification CIP-005 R1.2.1 to understand the reason for restricting management systems to only share CPU with other Management Systems. We recommend the language be revised to state that BCS can only share CPU with other BCS. Additionally, should CPU be shared across Management Systems for BCAs and Management Systems for Non-BES Cyber Assets? EEI request clarification on whether segmentation can be achieved through policies or does segmentation need to occur on separate physical blades (air gap)? CIP-005, Requirement R2, Part 2.2: states, “Protect the confidentiality and integrity (e.g., encryption) of IRA between the client and the Intermediate System.” EEI understands this to mean that encryption is only required between user/client and the IS and not between the IS and the BCS. In the substation remote access case the Intermediate System may be at a central location (Control Center/Data Center) and the link to the BCS may travel many miles over links owned by providers (i.e., telecom carriers). This appears to imply that not encrypting this communication is acceptable. This appears to be a gap that should be addressed or clarified.	
Likes 0	
Dislikes 0	

Response

Gladys DeLaO - CPS Energy - 1

Answer	
Document Name	

Comment

CPS Energy recommends revisions that do not drastically change the existing standards. Backwards compatibility is not evident in the revisions. Additonally, the attention given to virtualization feels over weighted compared to non-virtualized systems and may increase burden to entities.

Likes 0	
Dislikes 0	

Response

Trevor Tidwell - Trevor Tidwell - 1,3

Answer	
Document Name	

Comment

With the revisions to CIP-005 R1.5 and move to allow a zero trust model it is unclear in the revision what measure would meet this for a single device with its own logical isolation. The host may not have an IDS or application layer firewall. Would a host with AVAM used for CIP-007 R3 be sufficient to met this requirement?

We have a concern about CIP-010 R2.1. The monitoring would now expand in scope to R1.1.6 items. Items R1.1.1 through R1.1.5 are properties of a device and R1.1.6 is security settings applied to a device. One of these things are not like the others. So why does the monitoring have to include only the security settings in R1.1.6 but not the other CIP-005 or CIP-007 securty controls? We recommend striking R1.1.6 from being in scope for CIP-010 R2.1.

While the Implementation does allow for early adoption it is unclear if the requirements must be adopted all at once or if an entity can adopt part of the standards and have a staggered implementation. If such a staggered implementation is allowed then is there an order that some must be adopted first as others are dependent on the first?

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	
Document Name	

Comment

Request putting ‘Baseline configuration in the Standard somewhere to make the CIP-010 backwards compatible.

Likes 0

Dislikes 0

Response

Aaron Staley - Orlando Utilities Commission - 1

Answer

Document Name

Comment

Please see JEA coments, an individual response to my comment is not required.

Likes 0

Dislikes 0

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer

Document Name

Comment

N&ST believes that as drafted, CIP-005-8 Requirements R2 and R3 are contradictory. Specifically:

R2 Part 2.1, which mandates the use of an Intermediate System for IRA, applies to SCI with IRA hosting High or Medium Impact BCS or their associated, PCA, PACS, or EACMS. At the same time:

R3, originally developed for vendor remote access to EACMS and PACS, and which does NOT mandate the use of an Intermediate System, applies to SCI hosting EACMS or PACS associated with High or Medium impact BCS.

As written, both R2 and R3 would seem to apply to an SCI hosting, for example, EACMS associated with High Impact BCS.

N&ST also believes allowing “no IS” vendor remote access to SCI that happen to be hosting only EACMS and/or PACS (and their associated Management Modules) creates an unacceptable security risk. We believe that all vendor remote connections to ANY SCI should require the use of an Intermediate System if there’s a person typing on a keyboard at the vendor location. We believe, further, that this position is consistent with the SDT’s stated goal of addressing security risks associated with serial IRA.

N&ST believes these issues can be simply resolved by making the following changes: For R2 Parts 2.1, 2.4, and 2.5, revise "Applicability" so those parts apply to SCI hosting High or Medium Impact BCS or their associated PCA, PACS, or EACMS. Make the same applicability changes for Management Modules. For R3, delete ALL proposed changes. N&ST believes CIP-005-7 R3 already covers both virtual and physical EACMS and PACS as written.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
Although the acronyms for BCS, SCI, and BCSI are addressed at the beginning of the standards, ERCOT suggests all terms should be spelled out at the beginning of applicable requirement language because the requirement language is the most used and referenced part of a reliability standard. This will aid in readability. ERCOT appreciates the work to address virtualization. However, based on the differences in technology between legacy system and virtualized systems, the SDT should consider moving the virtualization requirements into a separate standard that addresses only the requirements applicable to virtualized environments. The SDT has received comments over time regarding the confusion that will be created by intermingling the legacy requirements and virtualization. If an entity has no intention of using virtualized systems, they may be confused by which requirements they should follow and how they would apply. In the purpose of CIP-013, "and their associated cyber systems" was added. Using "cyber systems" may lead to confusion and inconsistent applicability by using undefined terms.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization	
Answer	
Document Name	
Comment	
• **CIP-005, Requirement 1, Part 1.3** – the SDT proposes to eliminate the requirement to "Require inbound and outbound access permissions…and deny all other access by default." This, coupled with the elimination of the ESP and EAP concepts, increases the complexity of demonstrating where security starts and stops. What keeps the sprawl in check? Could the SDT describing their thinking on this in the Technical Rational document?	

- **CIP-005, Requirement 1, Part 1.5** – the proposed changes are problematic because an entity "must detect" as opposed to "having a method to detect." How can an entity know or demonstrate that they are able to detect *all* known or suspected malicious Internet Protocol communications?

Recommendation: SRC proposes the following lanuguage for Part 1.5: "**Have one or more method(s) for detecting** known or suspected malicious Internet Protocol (IP) communications…"

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	
Document Name	

Comment

In general, AWS supports the proposed requirements revisions to accommodate on-premises use of virtualization. Understanding that this SDT is focused on virtualization as it relates to on-premises, we read the revisions with the multiple uses of virtualization and emerging technologies in mind to consider language for both current and future applicability.

Comment #1

Virtualization technology provides powerful capabilities for logical separation. The Technical Rationale documentation makes clear that logical isolation methods are as effective as physical methods, including when used in mixed trust environments. The proposed requirements like those in CIP-005 R1 Part 1.2; CIP-005 R2 Part 2.6; and, CIP-010 R1 Part 1.1, do not differentiate or explicitly state that logical or physical isolation methods are acceptable, which we read as providing the Responsible Entities the flexibility to use either logical or physical isolation to meet the requirements. If this is the intent then a useful addition would be for the requirements to explicitly state this either with a universal, over-arching statement or within the requirement language.

Comment #2

The CIP-004 or CIP-011 requirements do not state that encryption of BCSI is sufficient in demonstrating prevention of unauthorized access of BCSI. It's important that the requirements are clear on this point, therefore we recommend that they explicitly state that individuals obtaining encrypted BCSI without the ability to use it within a meaningful timeframe should be considered as not having access. This is in accordance with the CMEP Practice Guide BES Cyber System Information. We recognize that a separate drafting team is addressing BCSI. We raise it here to encourage coordination and avoid unnecessary revision in the future.

Thanks to the SDT for the hard work to revise the requirement language and support adoption of technology in a secure and compliant manner.

Likes 0	
Dislikes 0	

Response	
Wayne Guttormson - SaskPower - 1	
Answer	
Document Name	
Comment	
Support the MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	
Document Name	
Comment	
CAISO signs on in support of SRC.	
Likes 0	
Dislikes 0	
Response	

Comments received from Paul Shipps – Lakeland Electric

1. The SDT added, revised, and retired several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

Definitions changes are extremely confusing and do not follow Industry standard terminologies. Many terminologies do not reference BES and hence its extemly confusing.

Further, most new definitions are not required and just BCS definition is sufficient. All other elements must follow, high watermarking and security controls and standards must apply.

2. CIP-005 Requirement R1 part 1.1 was revised to permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

There is no need to change a pre-established definition such as ESP. New application creates extreme confusion for application of security for cyber assets. Compartmentalization should be based on security enclaving but high water marking. A VLAN should be high water marked to Cyber Asset level as BES function will be impacted if it is compromised.

It seems SDT has compartmentalized assets in order to limit compliance application. Selective application of controls will result in significant security risks.

3. The SDT modified CIP-005 Requirement R1 Part R1.2 to establish logical isolation requirements for Management Systems, Management Interfaces, and associated SCI. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

System should continue to follow security model of complete distrust. Only communication that is required must be allowed. This can only be established if rules are explicit including, Source, destination, Ports and Protocol. New application is very subjective and confusing. Industry is currently using Goose and still compliant, why change configuration and standards must be technology neutral.

4. The SDT modified CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters. Does the proposed requirement fulfill the directive from FERC Order 791, paragraph 150? Please provide the basis for your response.

○ Yes

● No

Applicability section is confusing. Too much compartmentalization of devices and non-industry standard definition are not needed. BCS definitions should be updated to address logical assets and apply high water marking.

Current approach limits security with assumption that associated devices can be compromised externally, but BES impact must be considered if Cyber system is compromised and made unavailable.

5. The SDT modified CIP-005 Requirement R2 to ensure remote access management requirements align with the new and revised virtualization terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

"Ensure that authorized IRA is through an Intermediate System. " – Can we communicate through the firewall. Previous standard was accurate. New standard is subjective and will create confusion.

6. The SDT revised CIP-007 Requirement R1 Part 1.1 to shift the security objective from logical network accessible ports to services. The proposed revisions require Responsible Entities to enable only network accessible services that have been determined to be needed by the Responsible Entity. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

Unnecessary confusion. Previous standard language was sufficient for design of security controls and application. Revert to old standard, which industry has worked hard to standardize and create controls that have been effective.

7. CIP-010 Requirement R1 currently requires Responsible Entities to develop a baseline configuration, authorize changes to the baseline, and document the changes. The SDT proposes to revise Requirement R1 to remove the reference to baseline configurations. The proposed revisions require the authorization of changes to Operating System(s), firmware, commercially available open-source software, custom software, logical network accessible ports, security patches applied, and SCI configurations. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

SDT has created an uncalled for scenario where, they have removed Baselines but left the baseline elements intact, this is causing significant confusion amongst SME.

Requiring CM as method of compliance will set a serious challenge and will limit ability to secure system as CMs do not include security baseline information, only the proposed changes, but assessment are never included in CM, just a summary of results.

This whole approach will result in inaccurate and subjective application and often result in contention with compliance and auditors.

Current CIP-010 standards and requirements are matured and industry has made significant process developing good controls. There is absolutely no reason to change as these changes do not improve security but are detrimental.

8. The SDT modified CIP-010 Requirement R3 Part 3.3 to ensure that vulnerability assessments are performed prior to logically connecting Cyber Assets, VCA, and SCI. The revised requirement allows the use of remediation VLANs to perform active vulnerability assessments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

Too much compartmentalization based on non-industry standard definition. Please review NIST Publication 800-125 (virtualization guidelines) and apply controls, based on Terms such as Management Systems, Guest, Hosts, Network virtualization, Infrastructure virtualization (Mixed Trust, Resources sharing, high-watermarking) and similar guidance that is used by Industry, SME and vendors. SDT approach is complicated and confusing which will result in different interpretation by SMEs and ERO.

9. CIP-002-5.1a includes exemption 4.2.3.2, which exempted Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. In the development of conforming changes, the SDT determined that the exemption should be split into two distinct exemptions to adequately cover all cyber systems associated with conforming changes. The SDT established those conforming changes in proposed Exemptions 4.2.3.2 & 4.2.3.3. Do the changes clearly identify the exempted cyber systems? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

Many entities have virtualized systems and were compliant with CIP in recent audits. Please do not over complicate. Focus on security or where gaps exists. Only changes to BCS to include virtual environment and logical asset configuration is required.

10. BCS and SCI are mutually exclusive by definition, however SCI poses a significant reliability risk to the Bulk Electric System. The SDT considered the risks associated with SCI and revised CIP-002 Requirement R1 to include the identification of SCI in Parts 1.3, 1.4, and 1.5. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

BCSI requirements are sufficient as in CIP-004 and CIP-011. Entities are compliant and appropriate controls are available to secure BCSI in current version.

Shared storage housing active BCS data should not be allowed for mixed trust environments and introduces significant risk to BES.

Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based in security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.

11. In the current enforceable standards, there are no requirements that can be used to tie a non-identification of EACMS, PACS, and PCAs to a single requirement. The SDT revised CIP-002 to include the identification of SCI associated with EACMS, PACS, and PCAs to help address this issue within the virtualization scope of the current SAR. The proposed requirement could reduce possible non-compliance to a single issue if a Responsible Entity fails to properly identify SCI associated with EACMS, PACS, or PCAs. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

Based on comments above, these changes are confusion and are detrimental to security.

12. The SDT modified CIP-002 Attachment 1, Criterion 2.1 to align with a previously approved Request for Interpretation (RFI) regarding "shared BES Cyber Systems." The SDT modified the criterion to reference each discrete shared BCS. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based in security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.

13. The SDT made conforming changes to CIP-003 and CIP-004. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

Current standards are sufficient and these changes are cosmetic. No changes to CIP-004 is required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

14. The SDT modified the Applicable Systems column in CIP-006 to include SCI hosting PACs associated with Medium Impact BCS with ERC or IRA. The SDT made the proposed revisions to clarify the scope of requirements that apply when an entity implements serial IRA. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

● Yes

○ No

15. The SDT made conforming changes to CIP-008 and CIP-009. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

Current standards are sufficient and these changes are cosmetic. No changes to CIP-008 or 009 is required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

16. The SDT modified CIP-011 Requirement R2 part 2.1, which will allow cryptographic erasure in scenarios where BCSI can't be mapped to particular disks in virtualized storage. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

Current standards are sufficient and these changes are cosmetic. No changes to CIP-007 is required to address Virtualization. Only applicability section needs to be modified along with BCS definition.

Mixed trust environment should not be permitted for BCS.

BCSI requirements are sufficient as in CIP-004 and CIP-011. Entities are compliant and appropriate controls are available to secure BCSI in current version.

Term Shared BES Cyber System is confusing. Host sharing BCS system will have same impact on any of the guests and hence need for enclaving based in security impact. Compartmentalizing application of security will result in significant confusion and use of non-industry standards definitions is very misleading for security controls.

17. The SDT performed a review of the CIP Standards and determined that CIP Exceptional Circumstances could be applied to the following additional requirements: CIP-004-7 Requirement R2 Part 2.2, CIP-004-7 Requirement R3 Part 3.5, CIP-006-7 Requirement R1 Part 1.8, CIP-006-7 Requirement R1 Part 1.9, CIP-006-7 Requirement R2, CIP-010-5 Requirement Part 1.2, and CIP-010-5 Requirement R1 Part 1.3. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

○ Yes

● No

Current standards are sufficient and these changes are cosmetic. No changes to CIP-007 is required to address Virtualization. Only applicability section needs to be modified along with BCS definition

18. Implementation Plan: The SDT proposes an Implementation Plan that makes the revised CIP Standards and definitions effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order. However, the implementation plan allows a Responsible Entity to elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. Do you agree with this proposal? If you think an alternate effective date is needed, please provide a detailed explanation of actions and time needed.

● Yes

○ No

19. Please provide any additional comments for the SDT to consider, if desired.

Too much compartmentalization based on non-industry standard definition. Please review NIST Publication 800-125 (virtualization guidelines) and apply controls, based on Terms such as Management Systems, Guest, Hosts, Network virtualization, Infrastructure virtualization (Mixed Trust, Resources sharing, high-watermarking) and similar guidance that is used by Industry, SME and vendors. SDT approach is complicated and confusing which will result in different interpretation by SMEs and ERO.

1. SDT draft utilizes non-industry standards requirements and terminology and, will result in confusion and subjective and varying application. Recommend that SDT use Industry standard terminology such as NIST or PCI-DSS and security controls as laid out in such frameworks.

2. All definitions be contextualized in relation to BES application.

3. Furthermore, require standard requirements to apply control application based on risk to the systems based industry standard approaches such as high watermarking practices instead of compartmentalizing security controls based on every unique device types that SDT has identified.

4. SDT has summarily discarded Industry standard practices such as baselining but replaces with subjective terms such as hardening, which varies depending on environment and device types. Such a scenario will lead to different conclusions by the auditors and entity SME.

5. It has taken four years for the industry to standardize the security and baselining requirement. New approach discards all the work done so far and creates confusing set of expectations.

6. Further, In CIP-10, tracking hardening requirements in a change management tickets is incorrect approach as CM are for tracking activities and not performing assessments and compare of configurations.

Consideration of Comments

Project 2016-02 Modification to CIP Standards

Comments Received Summary

There were 91 sets of responses, including comments from approximately 210 different people from approximately 133 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact Vice President of Engineering and Standards Howard Gugel (via email) or at (404) 446-9693.

Consideration of Comments

The Project 2016-02 thanks all of industry for your time and comments.

NERC Glossary of Terms (Proposed new, modified, and retired terms)
Overall Themes concerning definitions in Q1 and SDT responses:

- Complex and difficult matrix of applicability that needs simplification
    - The SDT has made several changes in order to help simplify the "Applicable Systems" column in the standards.
- Wholesale changes are not needed, work virtualization into existing concepts with only a few virtualization specific terms needed.
    - The SDT continues to simplify and has incorporated this comment by making the "all-in scenario" possible where a virtualized infrastructure and all its components are all treated as part of its highest impact hosted BCS. This will greatly simplify and cause the least amount of changes for those using this scenario, while keeping other options open for other entities.
- Definitions are not limited in scope to virtualization only scenarios.
    - The SDT views the NERC Glossary the same as any dictionary with a purpose of simply defining what a term means, but not as a primary scoping mechanism for requirements within the standards. The glossary term and its definition should be able to be used across the NERC standards with differing scopes for different requirements, which can't be done if the scope is part of the definition.
- The changes are not applicable to cloud, hindering NERC's ability to move forward into cloud-based apps.

    - Enabling BES Cyber Systems to be hosted "in the cloud" on Cyber Assets outside of the entity's physical control is not included in the scope of our current SAR. The possibility of hosting BCS in the cloud is the subject of a forthcoming NERC report on the risks and benefits of such.

- The term "cyber system" has been added in exemptions and in requirements but is undefined.
    - The SDT agrees and is providing a proposed glossary definition in the next draft and will capitalize the term where used.
- "Controlled communications" and "System hardening" added and not defined
    - For 'controlled communications', the SDT is using that to mean that the communications are to be controlled and the remainder of the requirement defines what that 'control' means: permit necessary traffic and deny all other traffic. As an example, it's the opposite of 'uncontrolled communications' which would be traffic that does not pass through any type of access control (firewall as an EAP, zero trust policy mechanism, etc.). 'System hardening' is simply the label of a table in CIP-007 and is a common IT discipline term for reducing the attack surface of a computer system. In the next draft, one of the non-network-oriented controls will be moved to this requirement, so it will be broader than simply ports and services and 'system hardening' is a broader term.
- BCS definition modification is all that's needed for virtualization
    - The SDT is incorporating the ability to have an "all-in scenario" where all the virtualization infrastructure can be included as part of an entity's BCS in addition to allowing entities to identify it separately.
- Use the terms "virtual machine, hypervisor, virtualized host, virtualization, container" borrowed from NIST glossary
    - The SDT is using VCA and SCI in order to make some distinctions from the way others may use similar terms. For example, SCI is broader than just the software layer that virtualizes the underlay resources. It includes that, but also includes the hardware and storage controllers that share storage, as well as the management interface. We needed a more encompassing term than hypervisor alone in order to help simplify applicability. The SDT agrees with using "container" and see the response on the SCA definition comments below.
- Please clarify "Internet Protocol (IP)" as used in CIP-005 R1
    - The SDT is referring to the Internet Protocol (IP) as defined by DARPA in RFC 791 and upon which the term "TCP/IP" is based.

BCSI Definition

- "ESP names" was deleted as an example, suggest replacing with "logical isolation names"

  - The SDT deleted this because the term ESP was proposed for retirement in draft 1. In response to other stakeholder feedback, the ESP term will not be retired and this will be added back to the BCSI definition.

- The definition includes SCI, but not Management Modules or Management Interfaces.
  - The SDT agrees and has changed the nesting of these terms so that it is more all-inclusive.

Cyber Assets Definition

- Changed from plural to singular but still plural in the definition
  - The SDT agrees and will align with the currently approved definition, which is plural.
- The CA definition should not exclude SCI. SCI is a CA with a specific purpose.
  - The SDT concluded that to include SCI within the Cyber Asset definition would require a complete rewrite of that very foundational definition in a non-backward compatible way. A core issue is how the current CA definition is inclusive of all HW, SW, and data “in the device” and is problematic when the point of virtualization is to abstract and separate the 1:1 relationship of the HW from the OS/SW.

EACMS Definition

- Broaden EACMS to include and replace SCI
  - The SDT concluded that EACMS is already a very broad definition. Electronic access control is a function and as the future progresses towards Zero Trust or other architectures practically everything could become an EACMS. Additionally, the SDT is defining SCI separately so that its management interface which should be subjected to higher requirements for hypervisors hosting many BCS can be scoped to requirements without it also applying to every firewall and domain controller as an example.
- Excludes access control and monitoring to the BCS themselves, its now only to the logical isolation. Domain controllers, etc. could fall out of being EACMS if they aren’t directly related to “logical isolation”
  - The SDT agrees and will make changes to reincorporate this. When changing the “of the ESP or BES Cyber Systems” to “logical isolation of the BES Cyber Systems”, an unintended consequence was removing the BCS out of direct scope. Thanks for the comment and this will be addressed in draft 2.
- Should be singular, not plural (System, not Systems)
  - The SDT agrees with the point, but that is a change that would have a documentation only ripple effect through every entity’s CIP program. The SDT declines to make that change at this point.

ERC Definition

- Confusing (external to what?) without ESP reference – each BCS in a rack could have ERC to its neighbor in a highly segmented network. Meant to scope the external connectivity, not within a rack.
    - The SDT agrees. With architectures such as Zero Trust shrinking ESPs to ever more granular levels, it becomes increasingly less useful as the boundary for ERC. the SDT has changed ERC to clarify that 'external' in ERC is external to the asset containing the Cyber System, which fits better with its intended scoping use as well.
- The 'from' (CA or VCA) is irrelevant. Its founded in communication, not cyber assets.
    - The SDT agrees and has removed that from the definition. It was used in the previous draft to help define what "external" meant.
- If routable protocol is being used but not through an EACMS, its not ERC.
    - While true under the previous draft definition alone, the entity would still be required to meet CIP-005 R1 which would require an EACMS to protect the applicable BCS.
- Between ERC and EACMS, one says "controlling comms" and the other says "restricting IRA". What's the difference in controlling and restricting?
    - The SDT has redefined both definitions so they use neither term.

ESP/EAP Definitions

- High degree of support for not retiring
    - The SDT is proposing to keep and redefine ESP for draft 2 in response to comments. The new proposed definition is broadened to allow for single, static perimeters around a network segment or many, dynamic "perimeters" around a session in zero trust models.
- Traditional ESPs will be used by entities for many years to come
    - The SDT agrees that the static network segment-based perimeter model has no discernable end-of-life; it will co-exist with other models such as zero trust for the foreseeable future. The SDT proposed retirement of the ESP/EAP terms in order to be more architecture agnostic, but due to feedback is reinstating both terms with broadened definitions that can accommodate other architectures.

Intermediate System Definition

- Overly broad – could potentially label other EACMS as IS. A FW restricts IRA so is any FW an IS?
    - The SDT is modifying the proposed definition to reinstate that the restriction of IRA is "to only authorized users" which was not in the previous draft. The SDT asserts this should help with clarity around this issue.
- Address IS as its own applicable system without including it in with EACMS to allow for more granular controls for IS.

    - The SDT asserts that Intermediate Systems is its own definition such that it can be called out for specific, more granular requirements in CIP-005 R2. However, it is included as an EACMS such that it is included in all the other CIP standards that apply to associated EACMS. Otherwise, Intermediate Systems would have to be added as a separate item in all other applicability columns that apply to EACMS.
- Adjust definition to recognize it could be one or more EACMS used to restrict IRA.
    - The SDT agrees and has made this modification.
- Needs the "to authorized users". Can be read that all users must be restricted from using it.
    - The SDT agrees and has made this modification.

IRA Definition

- Need to clearly distinguish between 'engineering access' and operators operating through a system.
    - The SDT agrees and has reinstated the concept of IRA being from "outside of any of the responsible entity's ESPs".
- "outside the asset" – asset is undefined, does it mean CIP-002 R1 assets? "Outside the logical isolation" – unclear
    - The SDT agrees with providing clarity around the issue of "outside of what" and has reinstated the use of ESP.
- Not limited to routable protocol, includes all serial only comms. Huge scope increase with Intermediate System implications for serial only.
    - The SDT is incorporating clarity on IP to serial conversions that allow users to interact in real time with a serial-only device (and thus not within an ESP) that is accessible via routable protocol. The SDT is reinstating the "using a routable protocol" phrase to clarify that the user is using such a protocol, but also clarifying that accessing an applicable system through a subsequent IP to serial conversion is also IRA. The SDT asserts this clarifies that serial ONLY communications are not included.
- Does not need to remove "or other remote access technology" – if no 'client' then not IRA
    - The SDT also received comments on clarifying the meaning of remote access clients or technology. The SDT proposes that the addition of "user-initiated real-time access by a person" along with "from outside of the Responsible Entity's ESPs" helps clarify the definition of IRA.
- VLANs used for logical isolation and thus IRA could occur inside of what was the ESP.
    - The SDT agrees and has reinstated the ESP within the definition.
- Every time you connect to a CIP asset in the same logical isolation area, you are doing ERC.

  - The SDT is reinstating ESP in place of logical isolation and has modified the related definitions in accordance.

Logical Isolation

- Universal support for defining this as its critical to not only CIP-005 but numerous other definitions
  - The SDT agrees. Logical isolation is indeed a foundational concept and the SDT used the term in at least four different forms which restricted us from making one definition. In response to comments, the SDT has decided to reinstate and broaden the ESP definition and reinstate its use in place of logical isolation throughout the standards.
- Need to clarify the relationship of physical isolation and logical isolation
  - See above. The SDT is reinstating the ESP term in place of logical isolation.
- Is logical isolation that is part of a system (Windows FW) the same as logical isolation of the system? If so, that makes all comms to that Cyber Asset ERC.
  - The SDT agrees and has made several changes and clarifications, including the removal of the ‘logical isolation’ term. We’ve also changed CIP-005 R1 to state “Host-based firewalls (that only protect the host on which they reside) are not a sufficient control to meet this requirement.”

Management Interfaces Definition

- Include within BCS definition
  - The SDT is providing this as an option by including this definition within the SCI definition and then providing an “all-in” option where the SCI can be a part of the BCS.
- A relay control panel or on/off button could meet the definition. Is a local display ‘monitoring’?
  - The SDT agrees and has added an explicit exclusion to the definition.

Management Modules Definition

- Include within the SCI or BCS definition
- Need to define ‘autonomous subsystem’ or otherwise clarify that an internal RAID controller that is providing management and monitoring capability is or isn’t a mgt module.
- Is Wake On LAN a management module?
- Is a module part of a Cyber Asset or its own separate cyber asset?
- Should Management Modules be explicit in requiring PSPs?
  - In reference to all comments on Management Module definition, the SDT has decided to simplify and collapse Management Module and Management System into a new singular Management Interface definition and then have requirements for controlling the access to Management Interfaces.

Management Systems Definition

- Conflicts with SCI definition
- Appears to be a hypervisor, but straddles between virtual and non-virtual environments.
- Tools such as Ghost that image systems can meet this definition.
    - In reference to all comments on Management Systems definition, the SDT has decided to simplify and collapse Management Module and Management System into a new singular Management Interface definition and then have requirements for controlling the access to Management Interfaces.

PACS Definition

- Has an “or SCI” – can SCI by itself perform the PACS function?
    - The SDT agrees that normally SCI doesn’t perform the PACS function directly, but it can support the PACS function and the SDT did not want to preclude SCI in this instance from being able to be considered part of a PACS.

PCA Definition

- Makes virtualization untenable for smaller scales
    - The SDT agrees that these clarifications may require additional hypervisors in order to mitigate vulnerabilities of systems of differing impact levels sharing the same underlying hardware. The clarifications are intended to mitigate the risks of HW-based side channel or VM escape attacks from peer hosted VCAs on the same hypervisor. However, there is now an “all-in” option within CIP-002 that could help alleviate this issue.
- Not clear what is being ‘actively remediated’
    - The SDT has included this exclusion to account for remediation VLANs in which CAs or VCAs may boot in a logically isolated state, checked against policy and remediated (patched, AV updates, etc.), and then logically connected to their production network. While this automated process occurs, it may share CPU or memory with a BCS, but should not be reclassified as a PCA for that short time period of remediation.
- Is a serially connected device to a BCS now a PCA? Unclear from undefined ‘logical isolation’.
    - The SDT agrees and is reinstating a modified ESP definition.
- Is the exclusion necessary – it requires logical connection and therefore already excludes assets that are not logically connected
    - The SDT asserts the exclusion is necessary as a VCA that is being instantiated in a remediation VLAN and being checked against policy before its logically connected to a “production” network could still be sharing CPU/memory with a BCS on the same hypervisor for that brief time. The SDT asserts it should not be a PCA during the time it is being remediated simply due to this possibility.

Removable Media Definition

- How is this directly connected to a network? What's the difference in "a network not logically isolated from" and a PCA?
  - The SDT is reinstating the ESP definition and restoring the definition to its former approved state with the addition of SCI to the scope.
- Was PCA intentionally removed?
  - The SDT agrees and has reinstated PCA back into the RM definition.

Reportable CSI Definition

- The ''currently approved" doesn't match what is currently in the glossary
  - The SDT does not find any differences in the currently approved definition in our proposed document and the NERC glossary.
- Doesn't include Management Module/Management Interface (CSI definition as well)
  - The SDT agrees and has made changes in the definitions and their nesting that will include such in the next draft.

SCA Definition

- "isolated" interpreted in a network context
- Could include JRE
- Running containers can be mutable during runtime, thus fall out of the definition. Many comments on the 'immutable'
- No definition needed, use common IT terms, point CIP-010 R1 to 'application container repositories'
- Seems to allude to a software appliance/package such as a virtual FW or virtual router
  - The SDT agrees with numerous comments on the SCA definition and will not be proposing a separate definition in subsequent drafts but will instead refer to common IT terms ("application containers") in CIP-010 R1 as suggested.

SCI Definition

- Includes but conflicts with the Management System definition in the "and/or" of "initialize, deploy, and/or configure"
  - The SDT agrees and has consolidated this reference into a single instance in the "Management Interface" definition using the "and" conjunction.
- What is the scope of "share"? BCS shares resources with itself – is every physical standalone box SCI? Clarify that share is with something besides itself.

  - The SDT has modified the definition to include that SCI shares CPU and memory resources "with one or more Virtual Cyber Assets…" which should clarify this issue.
- Consider replacing SCI as high-watermarked BCA
  - The SDT has made modifications to CIP-002 to allow for such an "all-in" scenario where high-watermarked SCI can be included in a BCS, while still allowing the flexibility to identify the SCI separately. See discussion in CIP-002 Technical Rationale document.
- Virtual environments could reside within specified physical security zones thus eliminating the need for a Shared Cyber Infrastructure (SCI) definition
  - The SDT agrees that SCI must have physical security protections (per CIP-006 and CIP-003 for lows) and asserts that the SCI requires its own definitional term so that further requirements can be placed on electronic access to its management interface as one example.
- Modify CA to include entire virtualization HW infrastructure
  - The SDT concluded that would require a complete rewrite of this very foundational definition in a non-backward compatible way. A core issue is how the current CA definition is inclusive of all HW, SW, and data "in the device" and is problematic when the point of virtualization is to abstract and separate the 1:1 relationship of the HW and OS/SW.
- Modify EACMS and PACS to include underlying HW
  - The SDT has made the requested modification.
- Defines two types of objects – the hypervisor and the management system.
  - The SDT agrees it combines differing types of objects, including the shared HW itself, the hypervisor software, and the management interface as one and led to this being defined as an 'infrastructure' rather than a device. The SDT asserts this leads to more simplified applicability within the standards.
- Interpreting to mean totally separate storage array is needed if hosting any CIP asset
  - The SDT asserts a storage array that is sharing its storage resources with a BCS or associated system is within the CIP standards scope, however it does not mean that the storage array must be dedicated to only CIP systems.
- Scoping SCI 'software' - Is firmware on a server blade SCI?
  - The SDT has modified the SCI definition and asserts that the term software is included in the list of items that "share CPU and memory with one or more VCAs…" and is intended to refer to the hypervisor software.
- Doesn't include network services, but the proposed definition could include network devices
  - The SDT has purposefully not included within the SCI definition devices that share network resources, as that would include every network hub or switch as SCI, which is not the

  - intent. A network device, such as a switch, that is used to configure and isolate different VLAN network segments would become an EACMS, not SCI.

- Many CA’s could meet SCI definition. A video card is a programmable electronic device. It shares CPU and memory with the motherboard. RAID controllers share their storage resources with the CA they are installed in.
  - The SDT asserts that both SCI and “Cyber Assets” begin with the same “programmable electronic devices” phrasing which sets them both to the same level, thus since a video card isn’t considered its own Cyber Asset, it should not be SCI either. The SDT has made clarifications that SCI must share CPU and memory with one or more Virtual Cyber Assets which the SDT asserts will help with clarity.
- Could be recursive – the Management System used to configure SCI is SCI itself. Suggest splitting.
  - The SDT has removed the proposal for a Management System definition and has included that functionality in a modified “Management Interface” definition that the SDT asserts helps with clarity in this issue.

TCA Definition

- “not logically isolated” would include devices that are physically isolated
  - The SDT is reinstating the ESP definition which will help clarify this situation.

VCA Definition

- Clarify short-lived VMs. Is a VM image the VCA or the images spawned?
  - The SDT has defined Virtual Cyber Asset such that it begins with “A logical instance of…” to clarify that an executing instance is the intended target. Image files are not a VCA, but their handling is clarified in CIP-010.

NERC Reliability Standard CIP-005

Overall Themes and SDT responses:

1. Logical Isolation- Define and Clarify

    - The SDT thanks you for your many detailed comments on logical isolation. Logical isolation is indeed a foundational concept and the SDT used the term in at least four different forms which restricted us from making one definition. In response to comments, the SDT has decided to reinstate and broaden the ESP definition and reinstate its use in place of logical isolation throughout the standards.

2. EACMS and PACS- Clarity of use in requirements, - PACS or EACMS hosted on standalone hardware, relationship of virtual PACS and EACMS to SCI

    - The SDT thanks you for your comments on EACMS and PACS. In response to comments, the SDT have modified the Applicable Systems for the requirements in R1. Changes have also been made to the Requirements, and a new Requirement 1.3 created.

3. Needed and Controlled Communication- Define and Clarify

    - The SDT thanks you for your comments on needed and controlled communications. The SDT is using that to mean that the communications are to be controlled and the remainder of the requirement defines what that ‘control’ means: permit necessary traffic and deny all other traffic. As an example, it’s the opposite of ‘uncontrolled communications’ which would be traffic that does not pass through any type of access control (firewall as an EAP, zero trust policy mechanism, etc.).

4. Needed and Controlled Communication- Suggested changes - Identify needed communications and control permitted communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

    - The SDT thanks you for your comments on needed and controlled communications. The requirement has been rewritten to read “Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”

5. “Define and Clarify the term Group”

    - The SDT thanks you for your comments on the wording of Requirement 1.1. In response to comments, the SDT has rewritten the requirement to read “Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”

6. Clarify/simplify protocol IEC TR-61850-90-5 R-GOOSE
    - The SDT thanks you for your comments on the protocols listed in the requirement as examples. The requirement has been rewritten to remove the references and now reads “Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”
7. Backwards Compatibility
    - The SDT thanks you for your comments on backwards compatibility. In response to comments, the SDT has decided to reinstate and broaden the ESP definition. The requirement has been rewritten to read “Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”
8. Requirement 1.1 Overall - Changes to 1.1 not required, Keep the ESP Term
    - The SDT thanks you for your comments on R1.1. Logical isolation is indeed a foundational concept and the SDT used the term in at least four different forms which restricted us from making one definition. In response to comments, the SDT has decided to reinstate and broaden the ESP definition and reinstate its use in place of logical isolation throughout the standards.

CIP-005 Requirement R1 Part 1.2.

1. The SDT modified CIP-005 Requirement R1 Part R1.2 to establish logical isolation requirements for Management Systems, Management Interfaces, and associated SCI. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

- Clarity on if addition of SCI results in inclusion of associated systems
    - ▪ *The SDT thanks you for your comments and has made proposed changes to the Standard to address this confusion.*
- Clarity on applicable systems and expansion
    - ▪ *The SDT has made several changes in order to help simplify the “Applicable Systems” column in the standards.*
- Defined Term (Management Module) excludes SCI, applicable systems includes SCI of Management Systems
    - ▪ *In reference to all comments on Management Systems definition, the SDT has decided to simplify and collapse Management Module and Management System into a new singular*

  - *Management Interface definition and then have requirements for controlling the access to Management Interfaces.*

- Need definition of Logical Isolation
  - *The SDT thanks you for your many detailed comments on logical isolation. Logical isolation is indeed a foundational concept and the SDT used the term in at least four different forms which restricted us from making one definition. In response to comments, the SDT has decided to reinstate and broaden the ESP definition and reinstate its use in place of logical isolation throughout the standards.*
- Need clarification of requirements with applicable systems of EACMS
  - *The SDT thanks you for your comments on EACMS and PACS. In response to comments, the SDT has modified the Applicable Systems for the requirements in R1. Changes have also been made to the Requirements, and a new Requirement 1.3 created.*
- Use existing definition
  - *The SDT thanks you for your comments on R1.1. Logical isolation is indeed a foundational concept and the SDT used the term in at least four different forms which restricted us from making one definition. In response to comments, the SDT has decided to reinstate and broaden the ESP definition and reinstate its use in place of logical isolation throughout the standards.*
- Need better separation for requirements between SCI and non-SCI
  - *The SDT thanks you for your comments and has made proposed changes to the Standard to address this confusion.*
- Need clarity for backward compatibility
  - *The SDT thanks you for your comments on backwards compatibility. In response to comments, the SDT has decided to reinstate and broaden the ESP definition.*
- Need better examples in Measures
  - *The SDT thanks you for your comment. The SDT has included more examples within the measures of the proposed changes.*
- Need clarity on requirements with management modules of SCI
  - *In reference to all comments on Management Systems definition, the SDT has decided to simplify and collapse Management Module and Management System into a new singular Management Interface definition and then have requirements for controlling the access to Management Interfaces.*
- Management Modules should also apply to BCAs, PACS, and EACMS that are not on the SCI. Texas RE seeks clarification on whether management modules on current applicable BCAs, PACS, EACMS that are not on SCI are applicable to the CIP Requirements and Parts in the Applicable Systems column.

  - *In reference to all comments on Management Systems definition, the SDT has decided to simplify and collapse Management Module and Management System into a new singular Management Interface definition and then have requirements for controlling the access to Management Interfaces.*
- Need to protect physical systems of virtual systems
  - *The SDT has made the requested modification.*
- Need more clarity on "controlled communication"
  - *The SDT thanks you for your comments on needed and controlled communications. The requirement has been rewritten to read "Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement."*

CIP-005 Requirement R1 Part 1.3.

SAR Related

- Language would require protections between two PSPs within a substation. This extends the requirement to medium impact BES Cyber Systems even non virtualized ones, which is beyond the scope of the SAR.
- Including PACS is a problem as PACS are not required to be within a PSP.
- Define "communication networks".
- Communication Networks needs to be define per Order 791 paragraph 150.
- Beyond the scope of the SAR (failed to understand we are extending a single ESP). Recommendation to revert changes.
- Should be moved back to CIP-006.

The SDT thanks you for your comments. Based on this group of comments the SDT has made modifications to the proposed language in an attempt to alleviate the concerns related to changes that are outside the scope of the SAR.

Encryption

- Suggestion to require a minimum level of encryption.
- Encryption reference should be in measures.
- Provide clarity for the "confidentiality and integrity" verbiage.
- Specific technology examples should be added to the IG as was presented in the Webinars.
- Suggestion to add "equally effective logical protection".

- Specific protocols in the requirements area should be moved to the measures area.

The SDT thanks you for your comments. Based on the comments related to encryption technologies the SDT will ensure that technology examples are added to the IG where applicable. Additionally, we will review the usage of the encryption verbiage in the requirement to evaluate if it is better placed in the measures area. Lastly, the phrase “confidentiality and integrity” is commonly understood to mean that the use of cryptographic mechanism is required to protect the data traversing between the described endpoints.

Exclusion

- Rewording of CIP-012 exclusion since Real-time Assessment and Real-time Monitoring are not clearly defined.
- Suggest changing the exclusion to "time-sensitive protection or control functions" to enable all such protocols to be included.
- Remove GOOSE exclusion and describe the general requirements of a such a protocol to enable similar protocols to be excluded.
- Exclusion should be expanded to also exclude communication to a Control Center owned by other entities.
- Exclusion should include voice communication.

The SDT thanks you for your comments. The SDT has modified the verbiage of the exclusion to remove specific protocols and utilized more generic verbiage to describe these protocols and use cases. The exclusion concerns “…data while being transmitted between Control Centers *subject to CIP-012*” and CIP-012 excludes voice communication. This requirement part, which could overlap CIP-012, includes this “subject to CIP-012” exclusion simply to avoid double jeopardy.

Physical Controls

- Confidentiality and Integrity includes physical controls, so specifically stating physical controls is redundant.
- Is physical protection enough rather than logical protection? Hardened conduits as an example.
- Add evidence of physical controls in the measures since physical controls are listed as being acceptable in the requirement.

The SDT thanks you for your comments. The phrase “confidentiality and integrity” is commonly understood to mean that the use of cryptographic mechanism is required to protect the data traversing between the described endpoints, so the SDT feels that specifically identifying physical protections is appropriate. The SDT feels that physical controls are adequate to meet this requirement assuming that those controls are properly implemented and documented per the requirement and the associated measures which have been added to the most recent draft.

Applicability

- Applicable systems uses "or" instead of "and" and is not consistent with the rest of the standard.
- Applicability is confusing.
- Applicability column is hard to read.

The SDT thanks you for your comments. The SDT agrees that the applicability column should be more easily understood and therefore it has been significantly reworked in an effort to provide additional clarity in the most recent draft.

Others

- Limits security and assumes associated devices can be compromised externally.
- Confusion about requirement when equipment is entity owned vs third party owned.
- Requires significant modifications without indicating how these changes can be accomplished in a compliant way.
- Unclear how this improves security.

The SDT thanks you for your comments. The SDT disagrees with the assertion that the draft language limits security or does not improve the security of the BES. Multiple requirements have been added or modified in an effort to better protect virtualized systems and the infrastructure that hosts the virtualized infrastructure. This has historically been an area with no associated requirements and frequently overlooked by entities. While the draft language does require significant modifications for some entities to become or remain compliant, it is up to the entity to evaluate their environment, requirements, and architecture to best construct a compliant solution.

Reliability Standard CIP-005 Requirement R2

The comments provided by industry on the posting of CIP-005-8 R2 fell into several common themes:

1. The change in the IRA definition has left the term “system to system” undefined
    - The SDT thanks you for your comments. While the approved definition of IRA stated that it is not “system to system” communications, the SDT asserts that many entities have defined “system to system communications” within their existing compliance programs. If the SDT were to define “system to system” communications, this may conflict with those entities defined definitions
2. Entities suggested that the sequence of Requirement R2 Parts 2.1 to 2.3 be changed to Parts 2.2, 2.1, 2.3.
    - The SDT thanks you for your comments. The SDT has discussed a possible change in sequence however, it concluded that this change would result in unneeded additional administrative burden on entities.

3. The IRA definition – needs to be more precise to take into account where all connections are serial based. For example, in a totally serial based system, the HMI control consoles would be considered IRA, but none of the proposed CIP-005-8 Requirement R2 controls could be applied.
    - The SDT thanks you for your comments. The SDT agrees with your comments. The SDT has updated the definition of IRA to include the qualifier "*using a routable protocol*" so as to scope out the CIP-005 Requirement R2 controls for these types of systems
4. The proposed Intermediate System definition should be "an EACMS that restrict its IRA"
    - The SDT thanks you for your comments. The SDT agrees with your comments. The SDT has updated the definition of Intermediate System to "*One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users*"
5. PACS and EACMS should not be added to scope for IRA (CIP-005-8 Requirement R2 Part 2.1). EACMS also causes a "hall of mirrors" issue for Intermediate Systems (which are also EACMS)
    - The SDT thanks you for your comments. The SDT agrees some with your comments. The SDT has updated the proposed Applicable Systems of CIP-005 Requirement 2 Part 2.1 with the following additions:
        - *EACMS that enforces an ESP for the Applicable Systems in Part 1.1.*
        - *SCI identified independently supporting an Applicable System above*

      The SDT asserts that the addition of "*EACMS that enforces an ESP for the Applicable Systems in Part 1.1.*" (i.e. CIP-005-8 Requirement R1 Part 1.1) is needed to provide the appropriate level of protection for the integrity of the ESP
6. In the proposed CIP-005-8 Requirement R2 Part 2.1, the word "*Ensure*" is too absolute
    - The SDT thanks you for your comments. The SDT agrees some with your comments. The SDT has updated the wording of CIP-005 Requirement 2 Part 2.1 to "*Permit authorized IRA, if any, only through an Intermediate System*…."
7. For the proposed CIP-005-8 Requirement R2 Part 2.6, why is affinity needed for virtualized Intermediate Systems?
    - The SDT thanks you for your comments. The SDT asserts that some entities have architected their Intermediate Systems to allow remote users to connect directly from the Internet. The SDT asserts that this type of architecture dramatically increases the cyber-attack surface area beyond that which would be normally associated with an internal corporate / business cyber system. As a result, the SDT asserts that the affinity requirement for Intermediate Systems is needed to cover this type of situation.
8. In the proposed IRA definition, what is a "remote access client"?
    - The SDT thanks you for your comments. The SDT has updated the proposed definition of IRA to "*User-initiated real-time access by a person…*" to eliminate this confusion.

9. When and where is encryption required for IRA?

    - The SDT thanks you for your comments. The SDT asserts that the proposed wording of CIP-005-8 Requirement R2 Part 2.2 is clear enough such that these controls are only required between the client and the Intermediate System.

NERC Reliability Standard CIP-007

The comments provided by industry on the posting of CIP-007-7 fell into several common themes:

1. The clarity, and value of requirement language was questioned, as well as the security concern over dynamic port allocations and over broad port ranges, with the shift from logical network accessible ports to network accessible services.

    - The SDT thanks you for your comments and is working to modify the ports and services requirements to address multiple clarity and security concerns present in the original wording.

2. There were several comments that indicated that a disparity exists with respect to how the term “system hardening” is used throughout CIP-007-7.

    - The SDT thanks you for your comments, however the team feels that the term is consistently used throughout CIP-007-7 and does not intend to modify the use of the term. The SDT will likely incorporate additional discussion of system hardening in the forthcoming Implementation Guidance.

3. There were several comments that indicated that many of the changes were not backwards compatible, especially with respect to SCI.

    - The SDT thanks you for your comments and has identified a path forward that will allow entities to include SCI within a BCS, EACMS or PACS, or identify the SCI independently. The entity benefit to the former is simplicity, where Requirement Applicability is modified to allow entities to treat their SCI as just a part of a BCS, and therefor increasing the backwards compatibility of the proposed language. The entity benefit of the option to identify SCI independently is the increased flexibility in hosting systems of differing impact on one SCI.

NERC Reliability Standard CIP-010

The comments provided by industry on the posting of CIP-010-5 fell into several common themes:

1. Many of the comments dealt with the removal of the “baseline” from the requirement language in CIP-010 R1. Some suggested that there was a security concern in doing so, others simply asked for additional clarity in the change.

    - The SDT thanks you for your comments and has chosen to include a description of the use of the “baseline” concept within the measures of CIP-010. In taking this step the SDT hopes to provide the requested clarity. The SDT has chosen to respond to the comments suggesting a security concern over the authorization of the software that is initially installed on a system, by stating that this is not a requirement in the current version of CIP-010. The authorization required by CIP-010-4 is to changes to the current baseline, and therefore the initial authorization of the baseline is not a required step. While this is a positive security control, it is not required by CIP-010.

2. Many comments suggested that the SCI entries in the Applicability column were extremely confusing and difficult to understand.
   - The SDT thanks you for your comments, and agrees with the stated concerns, and has addressed this concern by simplifying both the Management related definitions down to one, and the SCI Applicability column insertions. These SCI Applicability column insertions as much simpler and the SDT hopes easier to understand by referring to the other Applicable Systems.
3. There were also many comments that provided feedback on unintended scope changes found within the proposed Requirement language.
   - The SDT thanks you for your feedback and has modified the Requirement language to reinstate the scope that was originally found within the language wherever possible. There still remain some aspects of the Standard that are not backwards compatible with respect to scope, but the SDT believes to have resolved each case of unintended scope change.
4. Many commenters suggested that the inclusion of Self-Contained Application (SCA) as a defined term, and to have is then appear within the scope of CIP-010 was unnecessary, as these should already have been included.
   - The SDT thanks you for your comments, and has removed the SCA as a defined term, and resolved to use the common term “application container” in its place. The reason the SDT chose to continue to include this term is to reinforce the concept that this is truly just software, and not to be construed as a Virtual Cyber Asset.
5. There were a number of commenters that suggested that inclusion of “images used to derive operating systems or firmware” in the Requirement language of CIP-010 is unnecessary since they should have been included already.
   - The SDT thanks you for your comments and has included the addition of “images used to derive operating systems or firmware” found in Requirement Part 1.1.1 to account for the concept of virtualized systems based on a “parent image.” These images may be updated separately from a derived virtual machine and become active as soon as the virtual machine is rebooted. In this case, changes to this parent image must follow the management requirements found in Requirement R1. The SDT asserts that while it may be included by implication, the inclusion provides needed clarity and focus around this scenario.
6. There were several comments that indicated a challenge with the shift to service, from ports, with respect to SCI, and that did not coincide with the shift in CIP-007.
   - The SDT has made changes to move SCI only Requirement language to a separate sub-part of R1, and coordinate ports and services language with the updated CIP-007 R1 Part 1.1 Requirement language.

7. There were also comments that indicated that the inclusion of SCI only requirement language within CIP-010 R1 Part 1.1 along with all the other portions caused confusion and created unintended challenges.
    - The SDT thanks you for your comments and has chosen move SCI only Requirement language to a new sub-part of CIP-010 R1.
8. There were also a few comments that indicated that the new CIP-010 R1 Part 1.1. change authorization requirement did not include a timing element.
    - The SDT thanks you for your comments and has chosen not to alter the Requirement language to include the timing element. This is consistent with the current version of CIP-010-4 and offers the most flexibility with respect to how an entity should implement this requirement. Additionally, this can be used to avoid the need for a CIP Exceptional Circumstance exception to the requirement, if an entity builds in an emergency change authorization concept to expedite these changes.

NERC Reliability Standards with Conforming Changes

1. Some commenters expressed concern regarding the conforming changes to the language for Exemptions 4.2.3.2 and 4.2.3.3 regarding cyber systems
    - The SDT agrees with your comments. The SDT has added a definition for Cyber System
2. Some commenters expressed concern regarding some of the conforming changes to CIP-002. They appear to be missing Management Modules. In addition, SCI is missing from Attachment 1, Criteria 2.1.
    - The SDT has modified the proposed definition of “Management Interface” so as to incorporate “Management Modules” into “SCI”. The SDT has also modified Attachment 1, Criterion 2.1 to incorporate SCI
3. Some commenters requested the SDT develop additional Technical Rationale.
    - The SDT updated the TR where necessary and encourages review of the updates.
4. Some commenters requested the SDT consider the addition of CEC in other respective areas of the CIP Standards.
    - The SDT thanks you for your comment and the current CEC changes are within the scope of our SAR. Overall changes to the CEC concept are outside the scope at this time.

Implementation Plan

There were some commenters who supported the 24 month implementation plan; however, some entities requested between 30 and 48 months. In addition, there were some requests for a phased-in/staggered implementation option.

- The SDT thanks you for your comments and has chosen not to change the implementation plan. 24-months should be sufficient time for the type of changes needed before becoming compliant. In addition, the SDT choose not to add a phased-in/staggered approach as the early adoption or two years should suffice.

Additional Comments Received

1. Some commenters asked the SDT to be consistent across the applicability columns.
    - The SDT focused on this during their draft 2 changes and the applicability columns are in a consistent state across the standards where applicable.
2. Some commenters expressed that more requirements were focused on virtualized assets versus physical assets.
    - The SDT charge for this project is to make modifications to clarify virtualized environments within CIP. There are additional requirements for virtualized systems due to the risks inherent in sharing underlying infrastructure (SCI) and access to the management interfaces that configure and control the SCI. These risks are not present with dedicated physical assets.
3. Some commenters expressed that virtualized environments can already be used and are not needed.
    - The SDT agrees that virtualization is allowed under the current CIP standards. The charge of this project is to provide additional clarity and to address risks from sharing cyber infrastructure. The SDT in draft 2 is including an “All-In” option which will preserve current state to a large degree for those with a dedicated virtualized environment where all parts are considered part of the BCS, but is allowing flexibility such that this is not the one prescribed way to treat SCI.
4. Some commenters expressed concern that the changes do not allow full backwards compatibility.
    - The SDT asserts that all modifications being made are being made with backwards compatibility in mind. For non-virtualized systems, backwards compatibility is being maintained with a few exceptions that are driven by security risks, such as protecting access to the Management Interfaces of EACMS that enforce ESPs
5. Some commenters expressed that there were too many modifications made to the standards.
    - The SDT thanks entities for this feedback and has reinstated terms such as ESP that have allowed draft 2 to revert a number of the draft 1 changes back to currently approved language. Note that the redlines posted with Draft 2 are against Draft 1 and thus do not reflect the degree of change from currently approved standards.
6. Some commenters expressed “change fatigue” and that the changes are administrative in nature.

- The SDT can't address concerns with the amount of version revisions by various SDTs. The SDT assumes that the comment on 'administrative changes' is due to the need to redefine all SCI in CIP-002 and treat is separately from the BCS it supports. The SDT has added flexibility in Draft 2 that allows for an "All-in" scenario that can help alleviate this concern.

7. Some commenters requested the GTB be inserted back into the standards.
    - The SDT thanks you for your comments; however, this is a NERC initiative across all standards and the GTB has been incorporated into technical rationale and implementation guidance respectively. Documents will be able to be accessed via the project page.
8. Some commenters acknowledged inconsistent format across all CIP Standards.
    - The SDT thanks you for your comments and has reviewed the standards to ensure format consistency across the CIP Standards.
9. Some commenters question the simultaneous posting between virtualization and BCSI projects.
    - The BCSI project has concluded and passed final ballot in June 2021. Draft 2 of the virtualization changes have been made to the final BCSI documents and now include those changes. BCSI was assigned a –X version number and virtualization a –Y version number. This allowed both projects to conclude a comment and ballot period during the same time and will assign correct version numbering upon completion of the projects.
10. Some commenters requested the SDT add identification of all systems to CIP-002.
    - The SDT reviewed and determined that adding identification of all systems (EACMS, PACS, PCA, etc.) is outside the scope of the SAR of this project.
11. Some commenters expressed concern regarding crossover from the standard modifications and the CMEP Practice Guides.
    - The SDT reviewed the respective CMEP practice guides. In addition, discussion was held with NERC compliance and determined that practice guides are used for currently enforceable standards and are reviewed as modified standards are completed and approved.

REMINDER
Standards Announcement
Project 2016-02 Modifications to CIP Standards

Initial Ballots and Non-binding Polls Open through March 22, 2021

Now Available

The initial ballots and associated Violation Risk Factors and Violation Severity Level non-binding polls for the **CIP Virtualization suite of standards (outlined below)** are open through **8 p.m. Eastern, Monday, March 22, 2021**.

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-9 - Cyber Security – Security Management Controls
- CIP-004-7 - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-3 - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Balloting
Use the Standards Balloting and Commenting System (SBS) to submit votes.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps
The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Applications" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box. For more information or assistance, Jordan Mallory (via email) or at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Formal Comment Period Open through March 22, 2021
Ballot Pools Forming through February 19, 2021

Now Available

A 60-day formal comment period for the **CIP Virtualization suite of standards (outlined below)** is open through **8 p.m. Eastern, Monday, March 22, 2021**.

- CIP-002-7 – Cyber Security - BES Cyber System Categorization
- CIP-003-9 – Cyber Security - Security Management Controls
- CIP-004-7 – Cyber Security - Personnel & Training
- CIP-005-8 – Cyber Security - BES Cyber System Logical Isolation
- CIP-006-7 – Cyber Security - Physical Security of BES Cyber Systems
- CIP-007-7 – Cyber Security - Systems Security Management
- CIP-008-7 – Cyber Security - Incident Reporting and Response Planning
- CIP-009-7 – Cyber Security - Recovery Plans for BES Cyber Systems
- CIP-010-5 – Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-011-3 – Cyber Security - Information Protection
- CIP-013-3 – Cyber Security - Supply Chain Risk Management

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. Contact Wendy Muller regarding issues using the SBS**.** An unofficial Word version of the comment form is posted on the project page**.**

Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Friday, February 19, 2021.** Registered Ballot Body members can join the ballot pools here. Note that there is a separate ballot and non-binding poll for each of the standards, so it is necessary to join each ballot pool in order to submit votes on all of the standards and their associated Violation Risk Factors and Violation Severity Levels.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Initial ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **March 12-22, 2021**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box. For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/212)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 IN 1 ST
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 277
Total Ballot Pool: 303
Quorum: 91.42
Quorum Established Date: 3/22/2021 3:18:47 PM
Weighted Segment Value: 38.97

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	25	0.368	43	0.632	0	8	10
Segment: 2	8	0.8	1	0.1	7	0.7	0	0	0
Segment: 3	67	1	19	0.328	39	0.672	0	5	4
Segment: 4	15	1	8	0.667	4	0.333	0	2	1
Segment: 5	72	1	22	0.393	34	0.607	0	8	8
Segment: 6	45	1	14	0.378	23	0.622	0	5	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	2	0.1	0	0	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	3	0.3	3	0.3	0	1	0
Totals:	303	6.5	92	2.533	154	3.967	0	31	26

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Third-Party Comments
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer		Abstain	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Calvin Wheatley		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Abstain	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	East Kentucky Power Cooperative	mark brewer		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Showing 1 to 303 of 303 entries

Previous 1 Next

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/212)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 IN 1 ST
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 276
Total Ballot Pool: 303
Quorum: 91.09
Quorum Established Date: 3/22/2021 3:33:37 PM
Weighted Segment Value: 48.44

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	33	0.485	35	0.515	0	8	10
Segment: 2	8	0.7	2	0.2	5	0.5	0	1	0
Segment: 3	67	1	25	0.431	33	0.569	0	5	4
Segment: 4	15	1	8	0.667	4	0.333	0	2	1
Segment: 5	72	1	27	0.482	29	0.518	0	7	9
Segment: 6	45	1	18	0.486	19	0.514	0	5	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	2	0.1	0	0	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	3	0.3	2	0.2	0	2	0
Totals:	303	6.3	116	3.052	128	3.248	0	32	27

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Third-Party Comments
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer		Abstain	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Calvin Wheatley		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	East Kentucky Power Cooperative	mark brewer		Affirmative	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 303 of 303 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/212)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 IN 1 ST
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 274
Total Ballot Pool: 301
Quorum: 91.03
Quorum Established Date: 3/22/2021 3:33:40 PM
Weighted Segment Value: 51.31

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	37	0.544	31	0.456	0	8	10
Segment: 2	8	0.7	2	0.2	5	0.5	0	1	0
Segment: 3	67	1	31	0.534	27	0.466	0	5	4
Segment: 4	14	1	8	0.727	3	0.273	0	2	1
Segment: 5	72	1	27	0.482	29	0.518	0	7	9
Segment: 6	44	1	16	0.444	20	0.556	0	5	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	2	0.1	0	0	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	3	0.3	2	0.2	0	2	0
Totals:	301	6.3	124	3.232	118	3.068	0	32	27

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Negative	Comments Submitted
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Third-Party Comments
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer		Abstain	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Calvin Wheatley		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	East Kentucky Power Cooperative	mark brewer		Affirmative	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/212)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 IN 1 ST
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 274
Total Ballot Pool: 301
Quorum: 91.03
Quorum Established Date: 3/22/2021 3:38:32 PM
Weighted Segment Value: 26.36

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	14	0.203	55	0.797	0	7	10
Segment: 2	8	0.8	0	0	8	0.8	0	0	0
Segment: 3	67	1	12	0.203	47	0.797	0	4	4
Segment: 4	14	1	6	0.545	5	0.455	0	2	1
Segment: 5	72	1	14	0.246	43	0.754	0	6	9
Segment: 6	44	1	8	0.216	29	0.784	0	4	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	2	0.1	0	0	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	3	0.3	3	0.3	0	1	0
Totals:	301	6.5	57	1.714	191	4.786	0	26	27

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Negative	Comments Submitted
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Third-Party Comments
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Wabash Valley Power Association	Calvin Wheatley		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	East Kentucky Power Cooperative	Patrick Woods		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
3	MEAG Power	Roger Brand		Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Negative	Comments Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Showing 1 to 301 of 301 entries

Previous 1 Next

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/212)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 IN 1 ST
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 274
Total Ballot Pool: 301
Quorum: 91.03
Quorum Established Date: 3/22/2021 3:34:03 PM
Weighted Segment Value: 42.81

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	26	0.4	39	0.6	0	11	10
Segment: 2	8	0.7	2	0.2	5	0.5	0	1	0
Segment: 3	67	1	22	0.386	35	0.614	0	6	4
Segment: 4	14	1	7	0.636	4	0.364	0	2	1
Segment: 5	72	1	24	0.429	32	0.571	0	7	9
Segment: 6	44	1	14	0.389	22	0.611	0	5	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	2	0.1	0	0	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	3	0.3	3	0.3	0	1	0
Totals:	301	6.4	98	2.74	141	3.66	0	35	27

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Negative	Comments Submitted
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Third-Party Comments
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer		Abstain	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Abstain	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Calvin Wheatley		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Abstain	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	East Kentucky Power Cooperative	mark brewer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/212)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 IN 1 ST
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 274
Total Ballot Pool: 301
Quorum: 91.03
Quorum Established Date: 3/22/2021 3:30:31 PM
Weighted Segment Value: 42.43

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	27	0.397	41	0.603	0	8	10
Segment: 2	8	0.8	1	0.1	7	0.7	0	0	0
Segment: 3	67	1	22	0.373	37	0.627	0	4	4
Segment: 4	14	1	8	0.727	3	0.273	0	2	1
Segment: 5	72	1	24	0.429	32	0.571	0	7	9
Segment: 6	44	1	16	0.432	21	0.568	0	4	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	2	0.1	0	0	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	3	0.3	3	0.3	0	1	0
Totals:	301	6.5	101	2.758	145	3.742	0	28	27

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Third-Party Comments
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer		Abstain	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Calvin Wheatley		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr.		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	mark brewer		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/212)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 IN 1 ST
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 274
Total Ballot Pool: 301
Quorum: 91.03
Quorum Established Date: 3/22/2021 3:34:05 PM
Weighted Segment Value: 52.87

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	37	0.561	29	0.439	0	10	10
Segment: 2	8	0.7	2	0.2	5	0.5	0	1	0
Segment: 3	67	1	32	0.561	25	0.439	0	6	4
Segment: 4	14	1	8	0.727	3	0.273	0	2	1
Segment: 5	72	1	28	0.509	27	0.491	0	8	9
Segment: 6	44	1	17	0.472	19	0.528	0	5	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	2	0.1	0	0	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	3	0.3	2	0.2	0	2	0
Totals:	301	6.3	127	3.331	111	2.969	0	36	27

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Third-Party Comments
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer		Abstain	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Abstain	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Calvin Wheatley		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Abstain	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	East Kentucky Power Cooperative	mark brewer		Affirmative	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Showing 1 to 301 of 301 entries

Previous 1 Next

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/212)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 IN 1 ST
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 273
Total Ballot Pool: 301
Quorum: 90.7
Quorum Established Date: 3/22/2021 3:41:42 PM
Weighted Segment Value: 53.26

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	38	0.576	28	0.424	0	10	10
Segment: 2	8	0.7	2	0.2	5	0.5	0	1	0
Segment: 3	67	1	32	0.561	25	0.439	0	6	4
Segment: 4	14	1	8	0.727	3	0.273	0	2	1
Segment: 5	72	1	28	0.519	26	0.481	0	8	10
Segment: 6	44	1	17	0.472	19	0.528	0	5	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	2	0.1	0	0	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	3	0.3	2	0.2	0	2	0
Totals:	301	6.3	128	3.355	109	2.945	0	36	28

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Third-Party Comments
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer		Abstain	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Abstain	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Calvin Wheatley		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Abstain	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	East Kentucky Power Cooperative	mark brewer		Affirmative	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/212)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 IN 1 ST
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 274
Total Ballot Pool: 301
Quorum: 91.03
Quorum Established Date: 3/22/2021 3:41:46 PM
Weighted Segment Value: 32.53

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	24	0.348	45	0.652	0	7	10
Segment: 2	8	0.8	0	0	8	0.8	0	0	0
Segment: 3	67	1	19	0.322	40	0.678	0	4	4
Segment: 4	14	1	6	0.545	5	0.455	0	2	1
Segment: 5	72	1	21	0.375	35	0.625	0	7	9
Segment: 6	44	1	12	0.324	25	0.676	0	4	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	2	0.1	0	0	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	2	0.2	4	0.4	0	1	0
Totals:	301	6.5	84	2.115	163	4.385	0	27	27

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Third-Party Comments
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Calvin Wheatley		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	East Kentucky Power Cooperative	Patrick Woods		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
3	MEAG Power	Roger Brand		Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	mark brewer		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/212)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 IN 1 ST
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 273
Total Ballot Pool: 301
Quorum: 90.7
Quorum Established Date: 3/22/2021 3:59:32 PM
Weighted Segment Value: 47.38

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	39	0.574	29	0.426	0	8	10
Segment: 2	8	0.8	0	0	8	0.8	0	0	0
Segment: 3	67	1	31	0.544	26	0.456	0	5	5
Segment: 4	14	1	8	0.727	3	0.273	0	2	1
Segment: 5	72	1	27	0.491	28	0.509	0	8	9
Segment: 6	44	1	16	0.444	20	0.556	0	5	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	2	0.1	0	0	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	3	0.3	3	0.3	0	1	0
Totals:	301	6.5	124	3.08	118	3.42	0	31	28

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Affirmative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Third-Party Comments
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer		Abstain	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Calvin Wheatley		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr.		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	East Kentucky Power Cooperative	mark brewer		Affirmative	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/212)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 IN 1 ST
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 273
Total Ballot Pool: 301
Quorum: 90.7
Quorum Established Date: 3/22/2021 4:07:57 PM
Weighted Segment Value: 51.37

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	35	0.538	30	0.462	0	11	10
Segment: 2	8	0.7	2	0.2	5	0.5	0	1	0
Segment: 3	67	1	31	0.544	26	0.456	0	5	5
Segment: 4	14	1	8	0.727	3	0.273	0	2	1
Segment: 5	72	1	27	0.482	29	0.518	0	7	9
Segment: 6	44	1	16	0.444	20	0.556	0	5	3
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	2	0.1	0	0	1	0.1	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	3	0.3	2	0.2	0	2	0
Totals:	301	6.3	122	3.236	116	3.064	0	35	28

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Third-Party Comments
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Abstain	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Bruce Reimer		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Third-Party Comments
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer		Abstain	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Preston Walker		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Negative	Third-Party Comments
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Calvin Wheatley		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Third-Party Comments
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Third-Party Comments
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Third-Party Comments
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	East Kentucky Power Cooperative	mark brewer		Affirmative	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Third-Party Comments
5	New York Power Authority	Shivaz Chopra		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Janet OBrien		Negative	Third-Party Comments
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Third-Party Comments
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Third-Party Comments
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	WEC Energy Group, Inc.	David Hathaway		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 | Non-binding Poll IN 1 NB
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 251
Total Ballot Pool: 277
Quorum: 90.61
Quorum Established Date: 3/22/2021 3:46:25 PM
Weighted Segment Value: 43.46

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	24	0.444	30	0.556	16	9
Segment: 2	8	0.6	1	0.1	5	0.5	2	0
Segment: 3	64	1	18	0.367	31	0.633	11	4
Segment: 4	14	0.9	8	0.8	1	0.1	4	1
Segment: 5	63	1	20	0.5	20	0.5	15	8
Segment: 6	40	1	10	0.37	17	0.63	9	4
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	2	0.1	0	0	1	0.1	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.5	2	0.2	3	0.3	2	0
Totals:	277	6.1	83	2.782	108	3.318	60	26

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Comments Submitted
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 277 of 277 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 | Non-binding Poll IN 1 NB
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 250
Total Ballot Pool: 277
Quorum: 90.25
Quorum Established Date: 3/22/2021 3:59:14 PM
Weighted Segment Value: 53.72

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	30	0.556	24	0.444	16	9
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	64	1	22	0.458	26	0.542	12	4
Segment: 4	14	0.9	8	0.8	1	0.1	4	1
Segment: 5	63	1	24	0.585	17	0.415	14	8
Segment: 6	40	1	14	0.538	12	0.462	10	4
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	2	0.1	0	0	1	0.1	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	277	5.9	101	3.238	87	2.662	62	27

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Comments Submitted
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Showing 1 to 277 of 277 entries

Previous 1 Next

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 | Non-binding Poll IN 1 NB
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 250
Total Ballot Pool: 277
Quorum: 90.25
Quorum Established Date: 3/22/2021 3:59:38 PM
Weighted Segment Value: 61.17

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	36	0.667	18	0.333	16	9
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	64	1	29	0.604	19	0.396	12	4
Segment: 4	14	0.9	8	0.8	1	0.1	4	1
Segment: 5	63	1	25	0.61	16	0.39	14	8
Segment: 6	40	1	14	0.538	12	0.462	10	4
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	2	0.1	0	0	1	0.1	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	277	5.9	115	3.519	73	2.381	62	27

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Showing 1 to 277 of 277 entries

Previous 1 Next

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 | Non-binding Poll IN 1 NB
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 248
Total Ballot Pool: 277
Quorum: 89.53
Quorum Established Date: 3/22/2021 4:09:03 PM
Weighted Segment Value: 29.32

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	14	0.264	39	0.736	15	11
Segment: 2	8	0.6	1	0.1	5	0.5	1	1
Segment: 3	64	1	12	0.25	36	0.75	12	4
Segment: 4	14	0.9	6	0.6	3	0.3	4	1
Segment: 5	63	1	14	0.333	28	0.667	13	8
Segment: 6	40	1	7	0.259	20	0.741	9	4
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	2	0.1	0	0	1	0.1	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.5	2	0.2	3	0.3	2	0
Totals:	277	6.1	56	2.007	135	4.093	57	29

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand		Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Comments Submitted
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 277 of 277 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 | Non-binding Poll IN 1 NB
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 248
Total Ballot Pool: 278
Quorum: 89.21
Quorum Established Date: 3/22/2021 4:09:11 PM
Weighted Segment Value: 48.37

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	26	0.52	24	0.48	18	12
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	64	1	20	0.426	27	0.574	13	4
Segment: 4	14	0.9	7	0.7	2	0.2	4	1
Segment: 5	63	1	21	0.512	20	0.488	14	8
Segment: 6	40	1	12	0.462	14	0.538	10	4
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	2	0.1	0	0	1	0.1	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.5	2	0.2	3	0.3	2	0
Totals:	278	6	89	2.919	95	3.081	64	30

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Abstain	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Comments Submitted
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Abstain	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 | Non-binding Poll IN 1 NB
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 248
Total Ballot Pool: 278
Quorum: 89.21
Quorum Established Date: 3/22/2021 4:09:15 PM
Weighted Segment Value: 48.17

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	26	0.491	27	0.509	15	12
Segment: 2	8	0.6	1	0.1	5	0.5	1	1
Segment: 3	64	1	20	0.408	29	0.592	11	4
Segment: 4	14	0.9	8	0.8	1	0.1	4	1
Segment: 5	63	1	22	0.537	19	0.463	14	8
Segment: 6	40	1	13	0.481	14	0.519	9	4
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	2	0.1	0	0	1	0.1	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.5	2	0.2	3	0.3	2	0
Totals:	278	6.1	92	3.017	99	3.083	57	30

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Comments Submitted
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 | Non-binding Poll IN 1 NB
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 248
Total Ballot Pool: 278
Quorum: 89.21
Quorum Established Date: 3/22/2021 4:09:16 PM
Weighted Segment Value: 62.84

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	36	0.706	15	0.294	17	12
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	64	1	29	0.617	18	0.383	13	4
Segment: 4	14	0.9	8	0.8	1	0.1	4	1
Segment: 5	63	1	25	0.625	15	0.375	15	8
Segment: 6	40	1	14	0.538	12	0.462	10	4
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	2	0.1	0	0	1	0.1	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	278	5.9	115	3.586	68	2.314	65	30

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Abstain	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Abstain	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 | Non-binding Poll IN 1 NB
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 247
Total Ballot Pool: 278
Quorum: 88.85
Quorum Established Date: 3/22/2021 4:11:20 PM
Weighted Segment Value: 62.64

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	35	0.7	15	0.3	17	13
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	64	1	29	0.617	18	0.383	13	4
Segment: 4	14	0.9	8	0.8	1	0.1	4	1
Segment: 5	63	1	25	0.625	15	0.375	15	8
Segment: 6	40	1	14	0.538	12	0.462	10	4
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	2	0.1	0	0	1	0.1	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	278	5.9	114	3.58	68	2.32	65	31

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Matt Lewis		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Abstain	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Abstain	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Showing 1 to 278 of 278 entries

Previous 1 Next

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 | Non-binding Poll IN 1 NB
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 248
Total Ballot Pool: 278
Quorum: 89.21
Quorum Established Date: 3/22/2021 4:09:25 PM
Weighted Segment Value: 38.74

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	21	0.396	32	0.604	15	12
Segment: 2	8	0.6	1	0.1	5	0.5	1	1
Segment: 3	64	1	16	0.327	33	0.673	11	4
Segment: 4	14	0.9	6	0.6	3	0.3	4	1
Segment: 5	63	1	19	0.463	22	0.537	14	8
Segment: 6	40	1	9	0.333	18	0.667	9	4
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	2	0.1	0	0	1	0.1	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.5	2	0.2	3	0.3	2	0
Totals:	278	6.1	74	2.42	117	3.68	57	30

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand		Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Comments Submitted
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Negative	Comments Submitted
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 | Non-binding Poll IN 1 NB
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 248
Total Ballot Pool: 278
Quorum: 89.21
Quorum Established Date: 3/22/2021 4:18:26 PM
Weighted Segment Value: 59.89

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	36	0.692	16	0.308	16	12
Segment: 2	8	0.6	1	0.1	5	0.5	1	1
Segment: 3	64	1	28	0.583	20	0.417	12	4
Segment: 4	14	0.9	8	0.8	1	0.1	4	1
Segment: 5	63	1	24	0.6	16	0.4	15	8
Segment: 6	40	1	13	0.5	13	0.5	10	4
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	2	0.1	0	0	1	0.1	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.5	2	0.2	3	0.3	2	0
Totals:	278	6.1	112	3.476	75	2.624	61	30

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Abstain	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 | Non-binding Poll IN 1 NB
Voting Start Date: 3/12/2021 12:01:00 AM
Voting End Date: 3/22/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 248
Total Ballot Pool: 278
Quorum: 89.21
Quorum Established Date: 3/22/2021 4:18:42 PM
Weighted Segment Value: 59.78

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	34	0.68	16	0.32	18	12
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	64	1	28	0.583	20	0.417	12	4
Segment: 4	14	0.9	8	0.8	1	0.1	4	1
Segment: 5	63	1	24	0.585	17	0.415	14	8
Segment: 6	40	1	13	0.5	13	0.5	10	4
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	2	0.1	0	0	1	0.1	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	278	5.9	110	3.449	74	2.451	64	30

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	ATCO Electric	Dan Bamber		Abstain	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Negative	Comments Submitted
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Renee Leidel		Negative	Comments Submitted
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Abstain	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Abstain	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Negative	Comments Submitted
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Randhir Singh		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Ginette Lacasse		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		None	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl		Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Abstain	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney		None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Negative	Comments Submitted
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Affirmative	N/A
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	John Allen		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Andrea Barclay		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		None	N/A
4	Sacramento Municipal Utility District	Foung Mua		Affirmative	N/A
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Avani Pandya		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Negative	Comments Submitted
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Abstain	N/A
5	Edison International - Southern California Edison Company	Neil Shockey		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Negative	Comments Submitted
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sacramento Municipal Utility District	Nicole Goi		Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Mickey Bellard		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Jerry Horner		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		None	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Abstain	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11 – June 24, 2021
45-day formal comment period with ballot	August 29–October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization
2. **Number:** CIP-002-7
3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the BES. Identification and categorization of BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.
4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. **Balancing Authority**

   4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-7:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See “Project 2016-02 Modification to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;

ii. Transmission stations and substations;

iii. Generation resources;

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;

v. RAS that support the reliable operation of the Bulk Electric System; and

vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Per Attachment 1, Section 1, identify each BES Cyber System as either of the following, if any, at each asset;

- A high impact BCS including any supporting SCI as part of the BCS; or
- A high impact BCS and independent SCI supporting any part of the high impact BCS or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).

1.2. Per Attachment 1, Section 2, identify each BES Cyber System as either of the following, if any, at each asset;

- A medium impact BCS including any supporting SCI as part of the BCS; or
- A medium impact BCS and independent SCI supporting any part of the medium impact BES Cyber System or its associated EACMS, PACS or PCAs.

1.3. Per Attachment 1, Section 3, identify any asset that contains a low impact BCS, or SCI that supports any part of a low impact BCS (a discrete list of low impact BCS or SCI that supports any part of a low impact BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS or independently identified SCI, five percent or fewer of identified BCS or independently identified SCI, have not	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS or independently identified SCI, more	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BCS or independently identified SCI, more than 10 percent but	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BCS or independently identified SCI, have not been categorized or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, five or fewer identified BCS or independently identified SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS or independently identified SCI, five percent or fewer high or medium BCS have not been identified; OR	than five percent but less than or equal to 10 percent of identified BCS or independently identified SCI, have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BCS or independently identified SCI, have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS or independently	less than or equal to 15 percent of identified BCS or independently identified SCI, have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BCA, more than 10 but less than or equal to 15 identified BCA have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS or independently identified SCI, more than 10 percent but less than or equal to 15	have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, more than 15 identified BCS or independently identified SCI have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS or independently identified SCI, more than 15 percent of high or medium impact BCS or independently identified SCI, have not been identified;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, five or fewer high or medium BCS or independently identified SCI, have not been identified.	identified SCI, more than five percent but less than or equal to 10 percent high or medium BCS or independently identified SCI, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, more than five but less than or equal to 10 high or medium BCS or independently identified SCI, have not been identified.	percent high or medium BCS or independently identified SCI, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, more than 10 but less than or equal to 15 high or medium BCS or independently identified SCI, have not been identified.	OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS or independently identified SCI, more than 15 high or medium impact BCS or independently identified SCI, have not been identified.
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous review. (Requirement R2 Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (Requirement R2 Part 2.2)	calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (Requirement R2 Part 2.2)	calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (Requirement R2 Part 2.2)	(Requirement R2 Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (Requirement R2 Part 2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Modification to CIP Standards Implementation plan”.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6		Criteria 2.12 Modifications Withdrawn	
7		Virtualization modifications.	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High Impact Rating**
   Each BCS used by and located at any of the following:

   1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

   1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

   1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

   1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium Impact Rating**
   Each BCS, not included in Section 1 above, associated with any of the following:

   2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are:

   - Each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection; or
   - Any SCI (which must be included in a shared BCS) supporting one or more BCS that together could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

   2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each RAS or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating, above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating

BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. RAS that support the reliable operation of the BES.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~initial~~ second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
~~45~~60-day formal comment period with ballot	January 21–~~February 8~~March 22, 2021
45-day formal comment period with ballot	June 30~~15~~ – ~~July 29~~August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	May 11 – June 24, 2021
45-day formal comment period with ballot	August ~~3~~29–~~September 16~~October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7~~5.1a~~

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those ~~BES Cyber Systems~~BCS could have on the reliable operation of the BES. Identification and categorization of ~~BES Cyber Systems~~BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

~~4.1.6.~~**4.1.5. Reliability Coordinator**

~~4.1.7.~~**4.1.6. Transmission Operator**

~~4.1.8.~~**4.1.7. Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~Special Protection System or Remedial Action Scheme~~RAS where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-7~~5.1a~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ Systems associated with communication ~~networks and data communication~~ links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See "Project 2016-02 Modification to CIP Standards Implementation Plan".

~~1. **24 Months Minimum –** CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

~~6. **Background:**~~

~~This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.~~

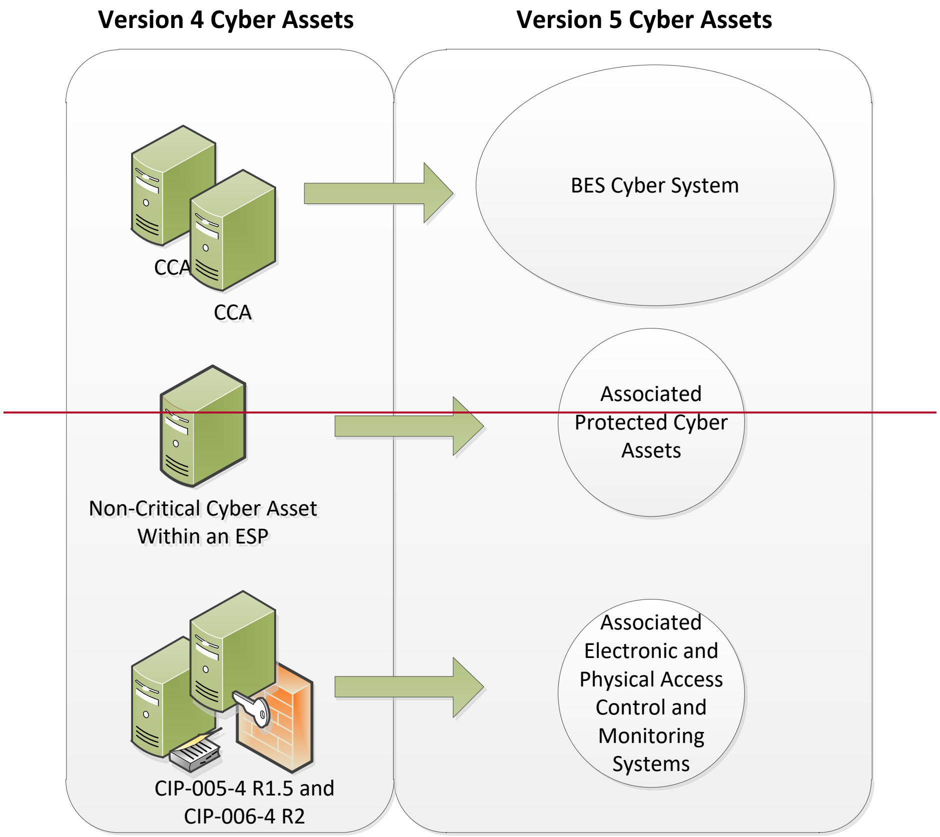
~~Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**BES Cyber Systems**~~

~~One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk~~

~~Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.~~



~~In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.~~

~~Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.~~

~~It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain~~

~~components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Reliable Operation of the BES~~

~~The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.~~

~~Real-time Operations~~

~~One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.~~

~~Categorization Criteria~~

~~The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.~~

~~This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.~~

~~**Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems**~~

~~BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:~~

> ~~**Electronic Access Control or Monitoring Systems ("EACMS")** – Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.~~
>
> ~~**Physical Access Control Systems ("PACS")** – Examples include: authentication servers, card systems, and badge control systems.~~
>
> ~~**Protected Cyber Assets ("PCA")** – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. ~~Special Protection Systems~~ RAS that support the reliable operation of the Bulk Electric System; and
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Per ~~Identify each of the high impact BES Cyber Systems according to~~ Attachment 1, Section 1, identify each BES Cyber System as either of the following, if any, at each asset;

- A high impact BCS including any supporting SCI as part of the BCS; or
- A high impact BCS and independent SCI supporting any part of the high impact BCS or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).

1.2. Per ~~Identify each of the medium impact BES Cyber Systems according to~~ Attachment 1, Section 2, identify each BES Cyber System as either of the following, if any, at each asset;~~ and~~

- A medium impact BCS including any supporting SCI as part of the BCS; or
- A medium impact BCS and independent SCI supporting any part of the medium impact BES Cyber System or its associated EACMS, PACS or PCAs.

1.3. Per ~~Identify each asset that contains a low impact BES Cyber System according to~~ Attachment 1, Section 3, identify any asset that contains a low impact BCS, or SCI that supports any part of a low impact BCS ~~if any~~ (a discrete list of low impact ~~BES Cyber Systems~~ BCS or SCI that supports any part of a low impact BCS is not required).

~~M2.~~M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1~~, and Parts 1.1 and 1.2~~.

R2. ~~The~~ Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

~~1.3.~~1.2. **Evidence Retention:**

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

~~1.4.~~1.3. **Compliance Monitoring and ~~Assessment Processes~~** Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~
- ~~Complaint~~

~~**1.5. Additional Compliance Information**~~

- ~~None~~

~~Table of Compliance Elements~~

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**High**	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact ~~BES Cyber Systems~~BCS or independently identified SCI, five percent or fewer of identified ~~BES Cyber Systems~~BCS or independently identified SCI, have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, five or fewer identified ~~BES Cyber Systems~~BCS or independently identified SCI have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, more than five percent but less than or equal to 10 percent of identified ~~BES Cyber Systems~~BCS or independently identified SCI, have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10	For Responsible Entities with more than a total of 100 high or medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, more than 10 percent but less than or equal to 15 percent of identified ~~BES Cyber Systems~~BCS or independently identified SCI, have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and ~~BES Cyber Assets~~BCA, more than 10 but less than or equal to 15	impact BES Cyber Systems, more than 15 percent of identified ~~BES Cyber Systems~~ BCS or independently identified SCI, have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, more than 15 identified ~~BES Cyber Systems~~ BCS or independently identified SCI have not been categorized or have been incorrectly categorized at a lower category.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, five percent or fewer high or medium ~~BES Cyber Systems~~ BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, five or fewer high or medium ~~BES Cyber Systems~~BCS or independently	identified ~~BES Cyber Systems~~BCS or independently identified SCI, have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, more than five percent but less than or equal to 10 percent high or medium ~~BES Cyber Systems~~BCS or independently identified SCI, have not been identified; OR	identified ~~BES Cyber Assets~~BCA have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, more than 10 percent but less than or equal to 15 percent high or medium ~~BES Cyber Systems~~BCS or independently identified SCI, have not been identified; OR For Responsible Entities with a total of	OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, more than 15 percent of high or medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, more than 15 high or medium impact ~~BES~~

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identified SCI, have not been identified.	For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, more than five but less than or equal to 10 high or medium ~~BES Cyber Systems~~BCS or independently identified SCI, have not been identified.	100 or fewer high and medium impact ~~BES Cyber Systems~~BCS or independently identified SCI, more than 10 but less than or equal to 15 high or medium ~~BES Cyber Systems~~BCS or independently identified SCI, have not been identified.	~~Cyber Systems~~BCS or independently identified SCI, have not been identified.
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (Requirement R2 Part 2.1)	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (Requirement R2 Part 2.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (Requirement R2 Part 2.2)	The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (Requirement R2 Part 2.2)	The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (Requirement R2 Part 2.2)	The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (Requirement R2 Part 2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- ~~None.~~See “Project 2016-02 Modification to CIP Standards Implementation plan”.

~~CIP-002-5.1a - Attachment 1~~

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating ~~(H)~~

Each ~~BES Cyber System~~BCS used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating ~~(M)~~

Each ~~BES Cyber System~~BCS, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only ~~BES Cyber Systems~~BCS that meet this criterion are:

- ~~those~~ Each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection; or
- Any SCI (which must be included in a shared BCS) supporting one or more BCS that together could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

~~2.1.~~2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~ each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

~~2.2.~~2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

~~2.3.~~2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

~~2.4.~~2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

~~2.5.~~2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

~~2.6.~~2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

~~2.7.~~2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

~~2.8.~~2.9. Each ~~Special Protection System (SPS), Remedial Action Scheme (~~RAS~~),~~ or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

~~2.9.~~2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

~~2.10.~~2.11. Each Control Center or backup Control Center, not already included in High Impact Rating ~~(H)~~ above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

~~2.11.~~2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating ~~(H)~~, above.

~~2.12.~~2.13. Each Control Center or backup Control Center, not already included in High Impact Rating ~~(H)~~ above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating ~~(L)~~

~~BES Cyber Systems~~BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. ~~Special Protection Systems~~ RAS that support the reliable operation of the ~~Bulk Electric System~~BES.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.~~

~~For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.~~

~~CIP-002-5.1a~~

~~CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset~~

~~includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."~~

~~The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:~~

~~Dynamic Response to BES conditions~~

~~Balancing Load and Generation~~

~~Controlling Frequency (Real Power)~~

~~Controlling Voltage (Reactive Power)~~

~~Managing Constraints~~

~~Monitoring & Control~~

~~Restoration of BES~~

~~Situational Awareness~~

~~Inter-Entity Real-Time Coordination and Communication~~

~~Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.~~

~~Entity Registration~~	**~~RC~~**	**~~BA~~**	**~~TOP~~**	**~~TO~~**	**~~DP~~**	**~~GOP~~**	**~~GO~~**
~~Dynamic Response~~		~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Balancing Load & Generation~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Controlling Frequency~~		~~X~~				~~X~~	~~X~~
~~Controlling Voltage~~			~~X~~	~~X~~	~~X~~		~~X~~
~~Managing Constraints~~	~~X~~		~~X~~			~~X~~	
~~Monitoring and Control~~			~~X~~			~~X~~	
~~Restoration~~			~~X~~			~~X~~	

~~Situation Awareness~~	~~X~~	~~X~~	~~X~~			~~X~~	
~~Inter-Entity coordination~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~	~~X~~

~~Dynamic Response~~

~~The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:~~

~~Spinning reserves (contingency reserves)~~

~~Providing actual reserve generation when called upon (GO,GOP)~~

~~Monitoring that reserves are sufficient (BA)~~

~~Governor Response~~

~~Control system used to actuate governor response (GO)~~

~~Protection Systems (transmission & generation)~~

~~Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)~~

~~Zone protection for breaker failure (DP, TO, TOP)~~

~~Breaker protection (DP, TO, TOP)~~

~~Current, frequency, speed, phase (TO,TOP, GO,GOP)~~

~~Special Protection Systems or Remedial Action Schemes~~

~~Sensors, relays, and breakers, possibly software (DP, TO, TOP)~~

~~Under and Over Frequency relay protection (includes automatic load shedding)~~

~~Sensors, relays & breakers (DP)~~

~~Under and Over Voltage relay protection (includes automatic load shedding)~~

~~Sensors, relays & breakers (DP)~~

~~Power System Stabilizers (GO)~~

~~Balancing Load and Generation~~

~~The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:~~

~~Calculation of Area Control Error (ACE)~~

~~Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)~~

~~Software used to perform calculation (BA)~~

~~Demand Response~~

~~Ability to identify load change need (BA)~~

~~Ability to implement load changes (TOP,DP)~~

~~Manually Initiated Load shedding~~

~~Ability to identify load change need (BA)~~

~~Ability to implement load changes (TOP, DP)~~

~~Non-spinning reserve (contingency reserve)~~

~~Know generation status, capability, ramp rate, start time (GO, BA)~~

~~Start units and provide energy (GOP)~~

~~Controlling Frequency (Real Power)~~

~~The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:~~

~~Generation Control (such as AGC)~~

~~ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)~~

~~Software to calculate unit adjustments (BA)~~

~~Transmit adjustments to individual units (GOP)~~

~~Unit controls implementing adjustments (GOP)~~

~~Regulation (regulating reserves)~~

~~Frequency source, schedule (BA)~~

~~Governor control system (GO)~~

~~Controlling Voltage (Reactive Power)~~

~~The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:~~

~~Automatic Voltage Regulation (AVR)~~

~~Sensors, stator control system, feedback (GO)~~

~~Capacitive resources~~

~~Status, control (manual or auto), feedback (TOP, TO,DP)~~

~~Inductive resources (transformer tap changer, or inductors)~~

~~Status, control (manual or auto), feedback (TOP,TO,DP)~~

~~Static VAR Compensators (SVC)~~

~~Status, computations, control (manual or auto), feedback (TOP, TO,DP)~~

~~Managing Constraints~~

~~Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:~~

~~Available Transfer Capability (ATC) (TOP)~~

~~Interchange schedules (TOP, RC)~~

~~Generation re-dispatch and unit commit (GOP)~~

~~Identify and monitor SOL's & IROL's (TOP, RC)~~

~~Identify and monitor Flow gates (TOP, RC)~~

~~Monitoring and Control~~

~~Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:~~

~~All methods of operating breakers and switches~~

~~SCADA (TOP, GOP)~~

~~Substation automation (TOP)~~

~~Restoration of BES~~

~~The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:~~

~~Restoration including planned cranking path~~

~~Through black start units (TOP, GOP)~~

~~Through tie lines (TOP, GOP)~~

~~Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)~~

~~Coordination (TOP, TO, BA, RC, DP, GO, GOP)~~

~~Situational Awareness~~

~~The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:~~

~~Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)~~

~~Change management (TOP,GOP,RC,BA)~~

~~Current Day and Next Day planning (TOP)~~

~~Contingency Analysis (RC)~~

~~Frequency monitoring (BA, RC)~~

~~Inter-Entity Coordination~~

~~The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:~~

~~Scheduled interchange (BA,TOP,GOP,RC)~~

~~Facility operational data and status (TO, TOP, GO, GOP, RC, BA)~~

~~Operational directives (TOP, RC, BA)~~

~~Applicability to Distribution Providers~~

~~It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.~~

~~Requirement R1:~~

~~**Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.**~~

~~**Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.**~~

~~Attachment 1~~

~~Overall Application~~

~~**In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.**~~

~~**When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.**~~

~~**In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.**~~

~~**It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities**~~

~~should formally agree on the designated Responsible Entity responsible for compliance with the standards.~~

~~High Impact Rating (H)~~

~~This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.~~

~~The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.~~

~~Additional thresholds as specified in the criteria apply for this category.~~

~~Medium Impact Rating (M)~~

~~Generation~~

~~The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.~~

~~Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing~~

~~**Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.**~~

~~**In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.**~~

~~**By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.**~~

~~**The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.**~~

~~**In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.**~~

~~**If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.**~~

~~**The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.**~~

~~**Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,** Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.**~~

~~**IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.**~~

~~**Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.**~~

~~**Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.**~~

~~**Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.**~~

~~Transmission~~

~~***The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.***~~

~~**Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems**~~

~~for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.~~

~~Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.~~

~~It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.~~

~~Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:~~

~~Excluded radial facilities that would only provide support for single generation facilities.~~

~~Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.~~

~~The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.~~

~~Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:~~

~~230 kV –> 700 MVA~~

~~345 kV –> 1,300 MVA~~

~~500 kV –> 2,000 MVA~~

~~765 kV –> 3,000 MVA~~

~~In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:~~

~~**For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.**~~

~~**Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.**~~

~~**Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.**~~

~~**Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.**~~

~~**The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.**~~

~~**The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.**~~

~~**The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.**~~

~~Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, Establish and Communicate System Operating Limits, R5.1.1 and R5.1.3.~~

~~Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.~~

~~Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.~~

~~Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.~~

~~Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.~~

~~This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value~~

~~of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.~~

~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.~~

~~Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.~~

~~Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Low Impact Rating (L)~~

~~BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.~~

~~Restoration Facilities~~

~~Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.~~

~~In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.~~

~~The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a~~

~~net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.~~

~~Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.~~

~~BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~

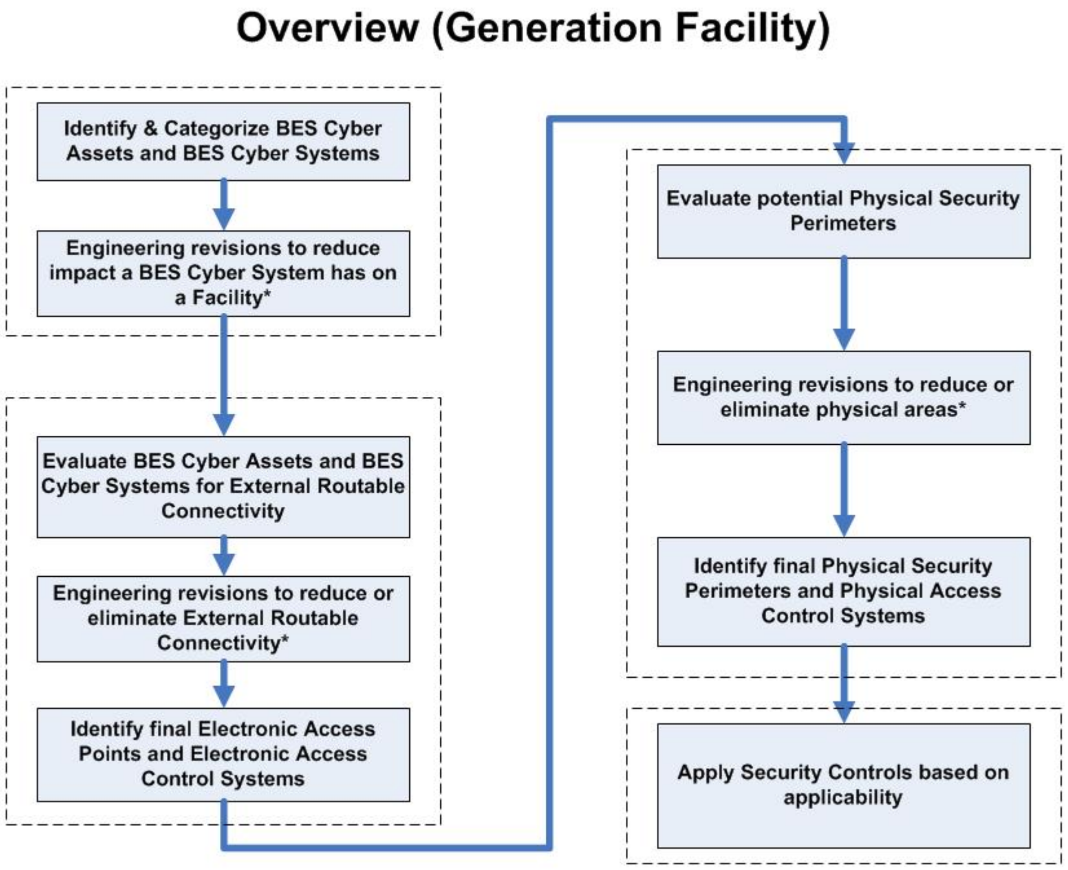
~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

~~BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.~~

~~Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.~~

~~Use Case: CIP Process Flow~~

~~The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.~~



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

~~Guidelines and Technical Basis~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for R1:~~

~~BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~Rationale for R2:~~

~~The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6		Criteria 2.12 Modifications Withdrawn	
7		Virtualization modifications.	

Appendix 1

~~Requirement Number and Text of Requirement~~

~~CIP-002-5.1, Requirement R1~~

~~R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:~~

~~Control Centers and backup Control Centers;~~

~~Transmission stations and substations;~~

~~Generation resources;~~

~~Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;~~

~~Special Protection Systems that support the reliable operation of the Bulk Electric System; and~~

~~For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.~~

~~Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;~~

~~Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and~~

~~Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).~~

~~Attachment 1, Criterion 2.1~~

~~Medium Impact Rating (M)~~

~~Each BES Cyber System, not included in Section 1 above, associated with any of the following:~~

~~Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~

~~Questions~~

~~Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."~~

~~The Interpretation Drafting Team identified the following questions in the RFI:~~

~~**Whether the phrase “shared BES Cyber Systems” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?**~~

~~**Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?**~~

~~**If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?**~~

~~**Responses**~~

~~Question 1: Whether the phrase “shared BES Cyber Systems,” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~

~~**The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states “Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…” Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states “*Each BES Cyber System*…associated with any of the following [criteria].” (emphasis added)**~~

~~**Additionally, the Background section of CIP-002-5.1 states that “[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System.” The Background section also provides:**~~

~~**The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.**~~

~~Question 2: Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~

~~**The phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple generation units.**~~

~~**The use of the term “shared” is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:**~~

~~**Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1:**~~ ~~Impact Rating of Generation Resource Shared BES Cyber Systems~~ ~~**for further information and examples.**~~

~~Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~**The phrase applies to each discrete BES Cyber System.**~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	August 29–October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-Y

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. Generator Operator

    4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-Y:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber Systems, associated with communication links, between Cyber Systems providing confidentiality and integrity of an

Electronic Security Perimeter (ESP) that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and SCI that supports any part of a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or SCI that supports any part of a low impact BCS is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS but did not address one of the nine topics required by Requirement R1. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS but did not address two of the nine topics required by Requirement R1. (Requirement R1 Part R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS but did not address three of the nine topics required by Requirement R1. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS but did not address four or more of the nine topics required by Requirement R1. (Requirement R1 Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Requirement R1 Part 1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months but did complete this review in less than or equal to 16 calendar months of the previous review. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	months but did complete this review in less than or equal to 17 calendar months of the previous review. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17	calendar months of the previous review. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 18

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (Requirement R1 Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS but did not address one of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified	calendar months of the previous approval. (Requirement R1 Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS but did not address two of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for	identified in CIP-002 containing low impact BCS but did not address three of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Requirement R1 Part 1.2) OR	calendar months of the previous approval. (Requirement R1 Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS but did not address four or more of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior	its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Requirement R 1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1 Part 1.2)	containing low impact BCS as required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Requirement R1 Part 1.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Requirement R1 Part 1.2)	the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Requirement R1 Part 1.2)		
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and SCI but failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and SCI but failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2)	The Responsible Entity documented the physical access controls for its assets containing low impact BCS and SCI but failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BCS and SCI according to Requirement R2, Attachment 1. (Requirement R2)

R #	**Time Horizon**	**VRF**	**Violation Severity Levels (CIP-003-Y)**			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and SCI but failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1,	OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and SCI but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and SCI but failed to document electronic access controls according to Requirement R2,	electronic access controls for its assets containing low impact BCS and SCI but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BCS and SCI but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Section 4. (Requirement R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BCS and SCI but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA	Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BCS, per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber	Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the introduction of malicious code for TCA	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			and Removable Media, but failed to manage its TCA according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	security plan(s) for its assets containing low impact BCS and SCI, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and SCI but failed to document the determination of whether an identified Cyber Security Incident is a	managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1,	implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to document mitigation for the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement the		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name,	The Responsible Entity has identified a delegate by name,	The Responsible Entity has identified a delegate by name, title, date of	The Responsible Entity has used delegated authority

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Modification to CIP Standards Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to

Version	Date	Action	Change Tracking
			identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BCS.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
Y	TBD	Virtualization conforming changes	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS or SCI that supports any part of a Low Impact BCS

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, (2) the asset or the locations of the SCI supporting low impact BCS within the asset, and (3) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BCS and each asset containing SCI that supports any part of a low impact BCS identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- an SCI that supports any part of a low impact BCS,

and a system(s) outside:

  - the asset containing the low impact BCS; or
  - the asset containing the SCI that supports any part of a low impact BCS; and

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or the asset containing the SCI that supports any part of a low impact BCS; and

iii. not used for time-sensitive protection or control functions between intelligent electronic devices.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports any part of a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, or SCI that supports any part of a low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the TCA to a low impact BCS or the SCI that supports any part of a low impact BCS (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports any part of a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code prior to connecting the Removable Media to a low impact BCS or SCI that supports any part of a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BCS or SCI that supports any part of a low impact BCS

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS or the SCI that supports any part of a low impact BCS within the asset; and
  b. The Cyber Asset(s), VCA, or SCI specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BCS, or SCI that supports any part of a low impact BCS, routable communication between a low impact BCS, or SCI that supports any part of a low impact BCS, and systems outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BCS, or SCI that supports any part of a low impact BCS, and systems outside the asset containing low impact BCS, or SCI that supports any part of a low impact BCS, or lists of implemented electronic access controls (e.g., access control lists

restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS or SCI that supports any part of a low impact BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, controls to maintain the known good state of the OS and software, application whitelisting practices, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of controls to maintain the

known good state of the OS and software, or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~initial~~ second draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
~~45~~60-day formal comment period with ballot	January 21–~~February 8~~March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~May 11–June 24, 2021~~
45-day formal comment period with ballot	August ~~3~~29–~~September 16~~October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-Y~~9~~

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-Y~~9~~:

4.2.3.1. Cyber ~~s~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~s~~Systems associated with communication links logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI).

4.2.3.3. Cyber ~~s~~Systems, associated with communication links, between Cyber ~~Assets~~Systems providing confidentiality and integrity of an Electronic Security Perimeter (ESP) ~~which~~ that ~~, Virtual Cyber Assets (VCA), or SCI performing logical isolation that~~ extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See "Project 2016-02 ~~Virtualization~~ Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS~~ and associated SCI~~, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS~~ and associated SCI~~, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and ~~their associated~~ SCI that supports any part of a low impact BCS, that

include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or ~~their associated~~ SCI that supports any part of a low impact BCS is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS ~~and associated SCI~~ but did not address one of the nine topics required by Requirement R1. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS ~~and associated SCI~~ as required by	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS ~~and associated SCI~~ but did not address two of the nine topics required by Requirement R1. (Requirement R1 Part R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS ~~and associated SCI~~ as required by	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS ~~and associated SCI~~ but did not address three of the nine topics required by Requirement R1. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS ~~and associated SCI~~ as required by Requirement R1 within 17 calendar months but did	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BCS ~~and associated SCI~~ but did not address four or more of the nine topics required by Requirement R1. (Requirement R1 Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS ~~and associated SCI~~ as required by Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS ~~and associated SCI~~ as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this	Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems BCS ~~and associated SCI~~ as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	complete this review in less than or equal to 18 calendar months of the previous review. (Requirement R1 Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS ~~and associated SCI~~ as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR	(Requirement R1 Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS ~~and associated SCI~~ as

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval in less than or equal to 16 calendar months of the previous approval. (Requirement R1 Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~and associated SCI~~ but did not address one of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its review	did complete this approval in less than or equal to 17 calendar months of the previous approval. (Requirement R1 Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~and associated SCI~~ but did not address two of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not	The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~and associated SCI,~~ but did not address three of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~and associated SCI~~ as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18	required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Requirement R1 Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~and associated SCI~~ but did not address four or more of the six topics required by Requirement R1. (Requirement R1 Part 1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~and associated SCI~~ as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002	complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~and associated SCI~~ as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Requirement R 1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for	calendar months of the previous review. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~and associated SCI~~ as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1 Part 1.2)	The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~and associated SCI~~ as required by Requirement R1. (Requirement R1 Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~and associated SCI~~ as required by Requirement R1 by

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			containing low impact BCS~~ and associated SCI~~ as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Requirement R1 Part 1.2)	its assets identified in CIP-002 containing low impact BCS~~ and associated SCI~~ as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Requirement R1 Part 1.2)		the CIP Senior Manager within 18 calendar months of the previous approval. (Requirement R1 Part 1.2)
R2	**Operations Planning**	**Lower**	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and ~~associated~~ SCI but failed to document cyber security awareness according	The Responsible Entity documented its cyber security plan(s) for its assets containing low impact~~-~~ BCS and ~~associated~~ SCI but failed to reinforce cyber security practices at least	The Responsible Entity documented the physical access controls for its assets containing low impact BCS and ~~associated~~ SCI but failed to implement the physical security controls according to Requirement R2,	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BCS and ~~associated~~ SCI according to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity implemented electronic access controls but failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and ~~associated~~ SCI but failed to document	once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for its assets containing low impact BCS and ~~associated~~ SCI but failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity documented its cyber security	Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls for its assets containing low impact BCS and ~~associated~~ SCI but failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for assets containing low impact	Requirement R2, Attachment 1. (Requirement R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BCS and ~~associated~~ SCI but failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1,	plan(s) for its assets containing low impact BCS and ~~associated~~ SCI but failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity documented its cyber security plan(s) for electronic access controls but failed to implement authentication for all Dial-up Connectivity that provides access to low impact BCS, per Cyber Asset capability according to Requirement R2, Attachment 1,	BCS and ~~associated~~ SCI but failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to manage its TCA according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA, but failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	Section 3.2 (Requirement R2) OR The Responsible Entity documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BCS and ~~associated~~ SCI, but failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented	The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				its cyber security plan(s) for its assets containing low impact BCS and ~~associated~~ SCI but failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable	Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Media, but failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to document mitigation for the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1,		

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Section 5.2. (Requirement R2) OR The Responsible Entity documented its plan(s) for TCA and Removable Media, but failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			the change. (Requirement R3)	50 calendar days of the change. (Requirement R3)		not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-Y~~9~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See "Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan."

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No.

Version	Date	Action	Change Tracking
			791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BCS.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding

Version	Date	Action	Change Tracking
			mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
Y~~9~~	TBD	Virtualization conforming changes	

Attachment 1

Required Sections for Cyber Security Plan(s) for Assets Containing Low Impact BCS ~~or their associatedand~~or SCI that supports any part of a Low Impact BCS

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, (2) the asset or the locations of the SCI ~~hosting~~ supporting low impact ~~BES Cyber Assets~~BCS within the asset, and (3) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BCS and each asset containing ~~or its associated~~ SCI that supports any part of a low impact BCS identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. ~~b~~Between:

- a low impact- BCS; or ~~and a system(s) outside the asset containing low impact BCS;~~
- ~~between~~ an SCI ~~hosting~~ that supports any part of~~ing~~ a low impact BCS,~~ and a system(s) outside the asset(s) containing the SCI hosting a low impact BCS;~~

and a system(s) outside:

- the asset containing the low impact BCS; or
- the asset containing the SCI that supports any part of~~ing~~ a low impact BCS; and

~~i.~~ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or ~~their associated~~ the asset containing the SCI that supports any part of~~ing~~ a low impact BCS; and

~~ii.~~iii. not used for time-sensitive protection or control functions between intelligent electronic devices~~ (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE)~~.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or ~~their associated~~ SCI that supports any part of a low impact BCS, per ~~Cyber Asset or VCA~~ system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, or ~~its associated~~ SCI that supports any part of~~ing~~ a low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;

- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the TCA to a low impact BCS or ~~its associated~~the SCI that supports any part of~~ing~~ a low impact BCS (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code ~~use of live operating system and software executable only from read-only media~~;
- Review of system hardening used by the party; or
- Review of ~~O~~other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or ~~its associated~~the SCI that supports any part of~~ing~~ a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code ~~on the Removable Media~~ prior to connecting the Removable Media to a low impact BCS or ~~its associated~~the SCI that supports any part of~~ing~~ a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BCS or ~~their associated~~the SCI that supports any part of~~ing~~ a low impact BCS

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS or ~~their associated~~the SCI that supports any part of~~ing~~ a low impact BCS within the asset; and
  b. The Cyber Asset(s), VCA, or SCI specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets containing low impact BCS, or SCI that supports any part of a low impact BCS, routable communication between a low impact BCS, or SCI that supports any part of a low impact BCS, and -systems outside the asset is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive protection or control functions between intelligent electronic devices. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) between the low impact BCS, or SCI that supports any part of a low impact BCS, and systems outside the asset containing low impact BCS, or SCI that supports any part of a low impact BCS, or

lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS or SCI that supports any part of a low impact BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, controls to maintain the known good state of the OS and software, application whitelisting practices, ~~processes to restrict communication,~~ or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update

process, the use of application whitelisting, ~~use of live operating systems~~use of controls to maintain the known good state of the OS and software, or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21– March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	August 29– October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 2021

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-Y

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-Y:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002-5.1a identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See "Project 2016-02 Modification to CIP Standards Implementation Plan"

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-Y Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-Y Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-Y Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS Medium Impact BCS SCI identified independently supporting an Applicable System above	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-Y Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-Y Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-Y Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium Impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BCSI and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-Y Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-Y Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-Y Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-Y Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-Y Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-X Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-X Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-Y Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-Y Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-Y Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access in a Physical Security Perimeter.

CIP-004-Y Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-Y Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-Y Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-Y Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-Y Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-Y Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-Y Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-Y Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BCS and their associated: - EACMS SCI identified independently supporting an Applicable System above	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: - Workflow or sign-off form showing password reset within 30 calendar days of the termination; - Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or - Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in *CIP-004-Y Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-Y Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-Y Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-Y Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-Y Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. **Compliance Enforcement Authority:** “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program:**
As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber security training program but failed to include four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-Y)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4)	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4)	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access	authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not

<table>
<tr><th rowspan="2">R #</th><th rowspan="2">Time Horizon</th><th rowspan="2">VRF</th><th colspan="4">Violation Severity Levels (CIP-004-Y)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td>authorization for one individual. (3.3 & 3.4)
OR
The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)</td><td>authorization for two individuals. (3.3 & 3.4)
OR
The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)</td><td>authorization for three individuals. (3.3 & 3.4)
OR
The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)</td><td>include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4)
OR
The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4)
OR
The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized</td></tr>
</table>

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (4.3)	necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (4.3)	necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (4.3)	unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (4.3)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (5.4) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances	termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the	termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the	unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)	predetermined date. (5.2)	predetermined date. (5.2)	authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)
R6	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6) OR The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.	more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	

Version	Date	Action	Change Tracking
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
~~45~~60-day formal comment period with ballot	January 21 ~~February 8~~– March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	August 29~~3~~– ~~September 16~~ October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 2021

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-Y~~X~~

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting ~~BES Cyber Systems~~BCS.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-Y~~X~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ Systems associated with communication ~~networks and data communication~~ links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~ BCS categorized as high impact or medium impact according to the CIP-002-5.1a identification and categorization processes.

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modification to CIP Standards Implementation Plan” ~~for CIP-004-X~~.

~~**Background:**~~

~~Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**"Applicable Systems" Columns in Tables:**~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-Y~~X~~ Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-Y~~X~~ Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-Y~~X~~ Table R1 – Security Awareness Program

Part	Applicable Systems	Requirements	Measures
1.1	High Impact ~~BES Cyber Systems~~BCS Medium Impact ~~BES Cyber Systems~~BCS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to ~~BES Cyber~~ Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-Y~~X~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-Y~~X~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-Y~~X~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of ~~BES Cyber System Information~~BCSI and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for ~~BES Cyber Systems~~BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with ~~a BES Cyber System's~~ electronic interconnectivity and interoperability with other Cyber ~~Assets~~Systems, including Transient Cyber Assets, and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-Y~~X~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to ~~applicable Cyber Assets~~Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

CIP-004-Y~~X~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to ~~BES Cyber Systems~~Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-~~X~~Y Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ Y Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~X~~ Y Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-~~X~~ Y Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-X Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-X Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ Y Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ Y Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~X~~ Y Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.1	High Impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access and unescorted physical access in a Physical Security Perimeter.

CIP-004-~~X~~ Y Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-~~X~~ Y Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-Y~~X~~ Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-Y~~X~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-Y~~X~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-~~X~~ Y Table R5 – Access Revocation			
Part	Applicable Systems	Requirements	Measures
5.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-~~X~~Y Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

5.4	High Impact ~~BES Cyber Systems~~BCS and their associated: - EACMS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: - Workflow or sign-off form showing password reset within 30 calendar days of the termination; - Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or - Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the “Applicable Systems” identified in *CIP-004-~~X~~ Y Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-~~X~~ Y Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-~~X~~ Y Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~X~~ Y Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-~~X~~ Y Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: - List of authorized individuals; - List of individuals who have been provisioned access; - Verification that provisioned access is appropriate based on need; and - Documented reconciliation actions, if any.
6.3	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact ~~BES Cyber Systems~~BCS with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an ~~a~~Applicable ~~s~~System above	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~Y)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15	The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)	security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar months of the previous training completion date. (2.3)		train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (R3) OR The Responsible Entity did conduct	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals,	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service	Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (3.2 & 3.4) OR	conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals. (3.1 & 3.4) OR The Responsible Entity has a process to perform

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	3.2.1 and 3.2.2 for two individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)	seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals. (3.3 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				(PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)		OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date. (3.5)
R4	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~Y)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for 5% or less of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (4.3)	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 5% but less than (or equal to) 10% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (4.3)	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 10% but less than (or equal to) 15% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (4.3)	access or unescorted physical access. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for more than 15% of its

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (4.3)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals. (5.3) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (5.1) OR The Responsible Entity has implemented one or more process(es) to	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals. (5.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one or more individuals. (5.4) OR The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (5.4)	determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)	The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (5.2)
R6	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for one individual, did not authorize provisioned electronic access to	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for two individuals, did not	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for three individuals, did not authorize provisioned	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (R6) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~Y)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 15 calendar months but less than or equal to 16 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for one individual, did not do so by the timeframe required in Requirement R6, Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 16 calendar months but less than or equal to 17 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned	electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 17 calendar months but less than or equal to 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but, for three individuals, did not do so by the timeframe	The Responsible Entity has implemented one or more program(s) as required by Requirement R6 Part 6.1 but, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (6.1) OR The Responsible Entity performed the verification required by Requirement R6 Part 6.2 more than 18 calendar months of the previous verification. (6.2) OR The Responsible Entity has implemented one or more program(s) to remove the individual's

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-~~X~~Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				access to BCSI but, for two individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.	required in Requirement R6, Part 6.3.	ability to use provisioned access to BCSI but, for four or more individuals, did not do so by the timeframe required in Requirement R6, Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to

Version	Date	Action	Change Tracking
			revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	August 29–October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-8

3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperations or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an Electronic Security Perimeter (ESP) that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See "Project 2016-02 Modification to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter(s)*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter(s)* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated Protected Cyber Asset (PCA) Medium Impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems such as: • Electronic Access Point (EAP) configuration or policies; • Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • SCI configuration or policies (hypervisor, fabric, backplane, or SAN configuration); that enforces an ESP and documents the business need.

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	Applicable Systems	Requirements	Measures
1.2	SCI identified independently supporting an Applicable System from Part 1.1. EACMS that enforces an ESP for the Applicable Systems in Part 1.1.	Permit only needed and controlled communications to and from Management Interfaces, and deny all other communications.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems that enforce access control and ESP such as: • Logical network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment), • Physically isolated out-of-band network for dedicated Management Interfaces, or • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3.	SCI identified independently supporting an Applicable System from Part 1.1.	Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems that enforce access control such as: • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration); • Logical network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated out-of-band network for dedicated Management Interfaces.

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS Medium Impact BCS at Control Centers	Protect the data traversing communication links used to span a single ESP between Physical Security Perimeters (PSP) through the use of: • confidentiality and integrity controls (such as encryption), or • physical controls that restrict access to the cabling and other nonprogrammable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and **ii.** time-sensitive protection or control functions between intelligent electronic devices.	An example of evidence may include, but is not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or policies used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI identified independently supporting an Applicable System above.	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.6	EACMS that enforces an ESP for the Applicable Systems in Part 1.1. at Control Centers	Detect known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. For all IRA and vendor remote access, excluding Dial-up Connectivity, the Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: • PCA Medium Impact BCS with ERC and their associated: • PCA EACMS that enforces an ESP for the Applicable Systems in Part 1.1. SCI identified independently supporting an Applicable System above Intermediate Systems used to access Applicable Systems of Part 2.1	Permit authorized IRA, if any, onlythrough an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, or Management Systems reports that show all IRA is through an Intermediate System.
2.2	Intermediate Systems used to access Applicable Systems of Part 2.1	Protect the confidentiality and integrity (e.g., encryption) of IRA between the client and the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents or configuration detailing where confidentiality and integrity controls initiate and terminate.

CIP-005-8 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.3	Intermediate Systems used to access Applicable Systems of Part 2.1	Require multi-factor authentication to the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-8 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.4	High Impact BCS with vendor remote access and their associated: • PCA Medium Impact BCS with vendor remote access and their associated: • PCA SCI identified independently supporting an Applicable System above	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including IRA and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BCS with vendor remote access and their associated: • PCA Medium Impact BCS with vendor remote access and their associated: • PCA SCI identified independently supporting an Applicable System above	Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including IRA and system-to-system remote access.
2.6	Intermediate Systems used to access Applicable Systems of Part 2.1	Implement for Applicable Systems as follows: **2.6.1.** Restrict VCAs of Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI. **2.6.2.** Permit only needed and controlled communications between Intermediate Systems and Applicable Systerms of Part 2.1.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Configuration showing that the CPU and memory can only be shared with other IS. Configuration showing how communications are controlled between the IS and applicable systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BCS EACMS and PACS associated with Medium Impact BCS with ERC SCI identified independently supporting an Applicable System above	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BCS EACMS and PACS associated with Medium Impact BCS with ERC SCI identified independently supporting an Applicable System above	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary,

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
			could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the ESP required by Part 1.1 or Part 1.2.2.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R1 – ESP*. (Requirement R1) OR The Responsible Entity did not permit only needed and controlled communications to and from applicable systems either individually or as a group and ESP all other communications. (Part 1.1) OR The Responsible Entity did not implement, for applicable systems, a method for restricting Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				capability (Requirement R1 Part 1.2.1) OR The Responsible Entity did not implement, for applicable systems, a method for permitting only needed and controlled communications to and from Management Interfaces and Management Systems, ESP all other communications. (Requirement R1 Part 1.2.2) OR The Responsible Entity did not implement, for applicable systems, a method for denying communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability (Requirement R1 Part 1.2.3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not implement a method to protect the data traversing communication links, where the ESP spans multiple Physical Security Perimeters, through the use of confidentiality and integrity controls (such as encryption); or physical controls that restrict access to the cabling and other nonprogrammable communication components (Requirement R1 Part 1.3) OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the applicable systems. (Requirement R1 Part 1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for	The Responsible Entity did not implement processes for one of the applicable	The Responsible Entity did not implement processes for two of the applicable	The Responsible Entity did not implement processes for three of the applicable

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Requirement Parts 2.1 through 2.3.	items for Requirement Parts 2.1 through 2.3.	items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Requirement R2 Part 2.4); or one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (Requirement R2 Part 2.5).	items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Requirement R2 Part 2.4) and one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (Requirement R2 Part 2.5). OR The Responsible Entity did not implement a method for applicable systems restricting Intermediate Systems to only share CPU and memory with its associated SCI and other Intermediate Systems, per

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				system capability (Requirement R2 Part 2.6.1) OR The Responsible Entity did not implement a method for applicable systems permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1 (Requirement R2 Part 2.6.2).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS, SCI, and Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for EACMS, SCI and	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS, SCI and Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote	The Responsible Entity did not implement any processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.2).	connections for EACMS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS, SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (Requirement R3 Part 3.2). OR The Responsible Entity had method(s) as required by Part 3.1 for PACS and EACMS but did not have a method to determine authenticated vendor-initiated remote connections for SCI or Management Modules of SCI (Requirement R3 Part 3.1).	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity had method(s) as required by Part 3.2 for PACS and EACMS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI or management Modules of SCI (Requirement R3 Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.”
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	
8	TBD	Virtualization modifications and ERC/IRA	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~initial~~ second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
~~45~~60-day formal comment period with ballot	January 21–~~February 8~~March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~May 11–June 24, 2021~~
45-day formal comment period with ballot	August ~~3~~29–~~September 16~~October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — ~~BES Cyber System Logical Isolation~~Electronic Security Perimeter(s)

2. **Number:** CIP-005-8

3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to ~~and from the system and logically isolating all other communication to~~ reduce the likelihood of misoperations or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber ~~s~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~s~~Systems associated with communication links ~~logically isolated from, but not providing logical isolation for, BCS or~~

~~Shared Cyber Infrastructure (SCI)~~between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber ~~s~~Systems, associated with communication links, between the Cyber ~~Assets~~Systems providing confidentiality and integrity of an Electronic Security Perimeter (ESP) that ~~, Virtual Cyber Assets, or SCI performing logical isolation that~~ extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~ part applies. ~~This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.~~

5. Effective Date: See "Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – ~~Logical Isolation~~Electronic Security Perimeter(s)*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter(s)~~Logical Isolation~~* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter(s)~~Logical Isolation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS ~~connected to a network via a routable protocol~~ and their associated ~~:~~ Protected Cyber Asset (PCA)~~;~~ ~~(VCA) Physical Access Control Systems (PACS) hosted on SCI; and~~ ~~Electronic Access Control or Monitoring System (EACMS) hosted on SCI~~ ~~•~~ Medium Impact BCS ~~connected to a network via a routable protocol~~ and their associated PCA~~:~~ ~~PCA;~~ ~~PACS hosted on SCI; and~~ ~~EACMS hosted on SCI~~	Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies ~~Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate~~ all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. ~~(e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).~~ Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems such as: • Electronic Access Point (EAP) configuration or policies; • Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • SCI configuration or policies (hypervisor, fabric, backplane, or SAN configuration); that enforces an ESP ~~electronic access control and logical isolation~~ and documents the business need.

CIP-005-8 Table R1 – Electronic Security Perimeter(s)~~Logical Isolation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	SCI identified independently ~~hosting~~supporting an Applicable System from Part 1.1. ~~High or Medium Impact BCS or their associated:~~ ~~• PCA;~~ ~~• PACS; or~~ ~~• EACMS~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PCA;~~ ~~• PACS; or~~ ~~• EACMS~~ EACMS that enforces an ESP for the Applicable Systems in Part 1.1. ~~perform logical isolation for a High Impact BCS~~ ~~EACMS that perform logical isolation for a Medium Impact BCS~~	~~Implement for applicable systems as follows:~~ ~~1.2.1. Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability.~~ ~~1.2.2.~~ Permit only needed and controlled communications to and from Management Interfaces, and ~~Management Systems, logically isolating~~deny all other communications. ~~1.2.3. Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.~~	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems that enforce access control and ESP~~logical isolation~~ such as: • Logical~~ly isolated out-of-band~~ network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment), • Physically isolated out-of-band network for dedicated Management Interfaces, or~~Management Modules, or Management Systems~~ • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter(s)~~Logical Isolation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3.	SCI identified independently supporting an Applicable System from Part 1.1.	Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems that enforce access control such as: • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration); • Logical network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated out-of-band network for dedicated Management Interfaces.

CIP-005-8 Table R1 – ~~Logical Isolation~~Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4~~3~~	High Impact BCS Medium Impact BCS at Control Centers ~~Impact BCS and their associated:~~ ~~PCA;~~ ~~PACS hosted on SCI; and~~ ~~EACMS hosted on SCI~~ ~~Medium Impact BCS connected to a network via routable protocol and their associated:~~ ~~PCA;~~ ~~PACS hosted on SCI; and~~ ~~EACMS hosted on SCI~~ ~~SCI connected to a network via routable protocol hosting High or Medium Impact BCS or their associated:~~ ~~PCA;~~ ~~PACS; or~~ ~~EACMS~~	Protect the data traversing communication links used to span a single ESP between ~~, where the logical isolationto spans a sindifferentmultiple~~ Physical Security Perimeters (PSP)~~,~~ through the use of: • confidentiality and integrity controls (such as encryption), or • ~~Physical~~ physical controls that restrict access to the cabling and other nonprogrammable communication components in those instances when such cabling and components are located outside of a ~~Physical Security Perimeter~~PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ~~i.~~ii. ~~excluding~~ time-sensitive protection or control functions between intelligent electronic devices. ~~(e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).~~	An example of ~~E~~evidence may include, but is not limited to, ~~architecture~~ documentations ~~detailing the~~of methods used to protect the confidentiality and integrity of the data, such as: ~~(e.g., encryption).~~ • Configurations or policies used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

CIP-005-8 Table R1 – ~~Logical Isolation~~Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.~~5~~4	High Impact BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI Medium Impact BCS with Dial-up Connectivity and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI SCI identified independently supporting an Applicable System above. ~~with Dial-up Connectivity hosting High or Medium Impact BCS or their associated:~~ ~~PCS;~~ ~~PACS; or~~ ~~EACMS~~	Perform authentication when establishing Dial-up Connectivity with ~~a~~Applicable ~~s~~Systems, per system capability.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-8 Table R1 – ~~Logical Isolation~~Electronic Security Perimeter(s)			
Part	Applicable Systems	Requirements	Measures
1.6~~5~~	EACMS that enforces an ESP for the Applicable Systems in Part 1.1. at Control Centers ~~High Impact BCS and their associated:~~ ~~PCA;~~ ~~PACS hosted on SCI; and~~ ~~EACMS hosted on SCI~~ ~~Medium Impact BCS at Control Centers and their associated:~~ ~~PCA;~~ ~~PACS hosted on SCI; and~~ ~~EACMS hosted on SCI~~ ~~SCI at Control Centers hosting High or Medium Impact BCS or their associated:~~ ~~PCA;~~ ~~PACS, or~~ ~~EACMS~~	Detect known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP ~~the logical isolation required by Part 1.1 or Part 1.2.2~~.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. For all IRA and vendor remote access, ~~that does not originate from applicable systems in Requirement R1 Part 1.1 or Part 1.2.2,~~ excluding Dial-up Connectivity ~~and TCAs~~, the Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: - PCA Medium Impact BCS with ~~Interactive Remote Access (IRA)~~ERC and their associated: - PCA EACMS that enforces an ESP for the Applicable Systems in Part 1.1. SCI identified independently supporting an Applicable System above ~~SCI with IRA hosting High or Medium Impact BCS or their associated:~~	~~Ensure that~~Permit authorized IRA, if any, only ~~is~~ through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, or Management Systems reports that show all IRA is through an Intermediate System.

	- ~~PCA;~~ - ~~PACS; or~~ - ~~EACMS~~ ~~Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PCA;~~ - ~~PACS; or~~ ~~EACMS~~		
2.2	Intermediate Systems used to access Applicable Systems of Part 2.1	Protect the confidentiality and integrity (e.g., encryption) of IRA between the client and the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents or configuration detailing where confidentiality and integrity controls initiate and terminate.
2.3	Intermediate Systems used to access Applicable Systems of Part 2.1	Require multi-factor authentication to the Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, - Something the individual knows such as passwords or PINs. This does not include User ID; - Something the individual has such as tokens, digital

			certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
2.4	High Impact BCS with vendor remote access and their associated: • PCA Medium Impact BCS with vendor remote access and their associated: • PCA SCI identified independently supporting an Applicable System above ~~SCI with vendor remote access hosting High or Medium Impact BCS or their associated:~~ ~~PCA~~ ~~Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated:~~ ~~PCA~~	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including IRA and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

2.5	High Impact BCS with vendor remote access and their associated: • PCA Medium Impact BCS with vendor remote access and their associated: • PCA SCI identified independently supporting an Applicable System abovee ~~SCI with vendor remote access hosting High or Medium Impact BCS or their associated:~~ ~~• PCA~~ ~~Management Modules with vendor remote access of SCI hosting High or Medium Impact BCS or their associated:~~ ~~PCA~~	Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including IRA and system-to-system remote access.
2.6	Intermediate Systems used to access ~~a~~Applicable ~~s~~Systems of Part 2.1	Implement for ~~a~~Applicable ~~s~~Systems as follows: **2.6.1.** Restrict VCAs of Intermediate Systems to only share CPU and memory with other	Examples of evidence may include, but are not limited to, documentation that includes the following: • Configuration showing that the CPU and memory can only be shared with other IS.

		Intermediate Systems and their associated SCI. **2.6.2.** Permit only needed and controlled communications between Intermediate Systems and ~~a~~Applicable ~~ms~~ Systerms of Part 2.1.	• Configuration showing how communications are controlled between the IS and applicable systems.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High Impact BCS EACMS and PACS associated with Medium Impact BCS with ~~External Routable Connectivity (~~ERC~~)~~ SCI identified independently supporting an Applicable System above ~~SCI hosting EACMS or PACS associated with High or Medium impact BCS~~ ~~Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS~~	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BCS EACMS and PACS associated with Medium Impact BCS with ERC	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	Applicable Systems	Requirements	Measures
	SCI identified independently supporting an Applicable System above ~~SCI hosting EACMS or PACS associated with High or Medium impact BCS~~ ~~Management Modules of SCI hosting EACMS or PACS associated with High or Medium impact BCS~~		systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the ~~logical isolation~~ESP required by Part 1.1 or Part 1.2.2.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R1 – ~~Logical Isolation~~ESP*. (Requirement R1) OR The Responsible Entity did not permit only needed and controlled communications to and from applicable systems either individually or as a group and ~~logically isolate~~ESP all other communications. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity did not implement, for applicable systems, a method for restricting Management Systems to only share CPU and memory with its associated SCI and other Management

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Systems, per system capability (Requirement R1 Part 1.2.1) OR The Responsible Entity did not implement, for applicable systems, a method for permitting only needed and controlled communications to and from Management Interfaces and Management Systems, ~~logically isolating~~ESP all other communications. (Requirement R1 Part 1.2.2) OR The Responsible Entity did not implement, for applicable systems, a method for denying communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability (Requirement R1 Part 1.2.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not implement a method to protect the data traversing communication links, where the ~~logical isolation~~ESP spans multiple Physical Security Perimeters, through the use of confidentiality and integrity controls (such as encryption); or physical controls that restrict access to the cabling and other nonprogrammable communication components (Requirement R1 Part 1.3) OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the applicable systems. (Requirement R1 Part 1.4)
R2.	The Responsible Entity does not have documented	The Responsible Entity did not implement processes	The Responsible Entity did not implement processes	The Responsible Entity did not implement processes

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.</td><td>for one of the applicable items for Requirement Parts 2.1 through 2.3.</td><td>for two of the applicable items for Requirement Parts 2.1 through 2.3;
OR
The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Requirement R2 Part 2.4); or one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (Requirement R2 Part 2.5).</td><td>for three of the applicable items for Requirement Parts 2.1 through 2.3;
OR
The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Requirement R2 Part 2.4) and one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (Requirement R2 Part 2.5).
OR
The Responsible Entity did not implement a method for applicable systems restricting Intermediate Systems to only share CPU and memory with its associated SCI and other</td></tr>
</table>

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				Intermediate Systems, per system capability (Requirement R2 Part 2.6.1) OR The Responsible Entity did not implement a method for applicable systems permit only needed and controlled communications between Intermediate Systems and applicable systems of Part 2.1 (Requirement R2 Part 2.6.2).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3)	The Responsible Entity had method(s) as required by Part 3.1 for EACMS, SCI, and Management Modules of SCI but did not have a method to determine authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.1). OR	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity had method(s) as required by Part 3.1 for PACS, SCI and Management Modules of SCI but did not have a method to determine authenticated vendor-	The Responsible Entity did not implement any processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS*. (Requirement R3) OR The Responsible Entity did not have any methods as

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The Responsible Entity had method(s) as required by Part 3.2 for EACMS, SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections for PACS (Requirement R3 Part 3.2).	initiated remote connections for EACMS (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS, SCI and Management Modules of SCI but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS (Requirement R3 Part 3.2). OR The Responsible Entity had method(s) as required by Part 3.1 for PACS and EACMS but did not have a method to determine authenticated vendor-initiated remote connections for SCI or Management Modules of	required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			SCI (Requirement R3 Part 3.1). OR The Responsible Entity had method(s) as required by Part 3.2 for PACS and EACMS but did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI or management Modules of SCI (Requirement R3 Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Virtualization Implementation Plan.”
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	
8	TBD	Virtualization modifications and ERC/IRA	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – August, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	August 29–October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 **Balancing Authority**

   4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 **Generator Operator**

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication links, between CyberSystems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See "Project 2016-02 Modification to CIP Standards Implementation Plan"

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.1	Medium Impact BCS without External Routable Connectivity (ERC) SCI without ERC hosting Medium Impact BCS Physical Access Control Systems (PACS) associated with: • High Impact BCS • Medium Impact BCS with ERC SCI, identified independently supporting an Applicable System above, not included in the Applicable Systems of Part 1.2 or Part 1.3	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI, identified independently supporting an Applicable System above, not included in the Applicable Systems of Part 1.3	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, per system capability.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.
1.5	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident response plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	Physical Access Control Systems (PACS) associated with: - High Impact BCS, or Medium Impact BCS with ERC SCI identified independently supporting an Applicable System above	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.
1.7	Physical Access Control Systems (PACS) associated with: - High Impact BCS, or - Medium Impact BCS with ERC SCI identified independently supporting an Applicable System above	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident response plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.
1.9	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2.	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with EERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BCS • Medium Impact BCS with ERC • SCI identified independently supporting a High Impact BCS; or • SCI identified independently supporting a Medium Impact BCS with ERC Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BCS • Medium Impact BCS with ERC • SCI identified independently supporting a High Impact BCS; or • SCI identified independently supporting a Medium Impact BCS with ERC	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Requirement R1 Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Requirement R1 Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Requirement R1 Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Physical Security Perimeter. (Requirement R1 Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (Requirement R1 Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (Requirement Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Requirement R1 Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Requirement R2 Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Requirement R2 Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (Requirement R3 Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (Requirement R3 Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Modification to CIP Standards Implementation Plan”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to

Version	Date	Action	Change Tracking
			use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes and CEC language added	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the initial draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
~~45~~60-day formal comment period with ballot	January 21–~~February~~ March ~~8~~22, 2021
45-day formal comment period with ballot	June 30 – August, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	May 11–June 24, 2021
45-day formal comment period with ballot	August ~~3~~29–~~September 16~~October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1 **Balancing Authority**

      4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

            4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

      4.1.3 **Generator Operator**

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-7:

4.2.3.1 Cyber ~~s~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~s~~Systems associated with communication links between discrete Electronic Security Perimeters (ESP)

~~logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI)~~.

4.2.3.3 Cyber ~~s~~Systems, associated with communication links, ~~that are~~ between Cyber ~~Assets~~Systems~~, Virtual Cyber Assets (VCA), or SCI performing logical isolation that~~ providing confidentiality and integrity of an ESP ~~which~~that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~ part applies. ~~This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.~~

5. Effective Dates: See “Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BCS without External Routable Connectivity (ERC) SCI without ERC hosting Medium Impact BCS Physical Access Control Systems (PACS) associated with: • High Impact BCS • Medium Impact BCS with ERC SCI, identified independently supporting an Applicable System above, not included in the Applicable Systems of Part 1.2 or Part 1.3 ~~• SCI hosting High Impact BCS or their associated EACMS or PCA; or~~ ~~• SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA~~ ~~SCI hosting PACS associated with High Impact BCS~~ ~~SCI hosting PACS associated with Medium Impact BCS with ERC~~	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI, identified independently supporting an Applicable System above, not included in the Applicable Systems of Part 1.3 ~~SCI with ERC hosting Medium Impact BCS or their associated:~~ ~~• EACMS; or~~ ~~• PCA~~	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS or their associated:~~ ~~• EACMS; or~~ ~~• PCA~~	Utilize two or more different physical access controls (this does not require two completely independent PACS~~physical access control systems~~) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, per system capability.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS or their associated:~~ - ~~EACMS; or~~ - ~~PCA~~ ~~SCI with ERC hosting Medium Impact BCS or their associated:~~ - ~~EACMS; or~~ ~~PCA~~	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-7 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.5	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS or their associated:~~ - ~~EACMS; or~~ - ~~PCA~~ ~~SCI with ERC hosting Medium Impact BCS or their associated:~~ - ~~EACMS; or~~ - ~~PCA~~	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the ~~BES~~ Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident response plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BCS, or ~~•~~ Medium Impact BCS with ERC ~~• SCI hosting High Impact BCS or their associated EACMS or PCA; or~~ ~~SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA~~ SCI identified independently supporting an Applicable System above ~~SCI hosting PACS associated with High Impact BCS~~ ~~SCI hosting PACS associated with Medium Impact BCS with ERC~~	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BCS, or • Medium Impact BCS with ERC ~~• SCI hosting High Impact BCS or their associated EACMS or PCAs; or~~ ~~• SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA~~ SCI identified independently ~~hosting~~supporting an Applicable System above ~~SCI hosting PACS associated with High Impact BCS~~ ~~SCI hosting PACS associated with Medium Impact BCS with ERC~~	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the ~~BES~~ Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident response plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS or their associated:~~ ~~• EACMS; or~~ ~~• PCA~~ ~~SCI with ERC hosting Medium Impact BCS or their associated~~ ~~• EACMS; or~~ • ~~PCA~~	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BCS and their associated: 1. EACMS; and 2. PCA ~~-~~Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS or their associated:~~ ~~• EACMS; or~~ ~~• PCA~~ ~~SCI with ERC hosting Medium Impact BCS or their associated:~~ ~~• EACMS; or~~ • ~~PCA~~	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS or their associated:~~ - ~~EACMS; or~~ - ~~PCA~~ ~~SCI with ERC hosting Medium Impact BCS or their associated:~~ - ~~EACMS; or~~ - ~~PCA~~	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with EERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS or their associated:~~ - ~~EACMS; or~~ - ~~PCA~~ ~~SCI with ERC hosting Medium Impact BCS or their associated:~~ - ~~EACMS; or~~ - ~~PCA~~	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS or their associated:~~ ~~• EACMS; or~~ ~~• PCA~~ ~~SCI with ERC hosting Medium Impact BCS or their associated:~~ ~~• EACMS; or~~ • ~~PCA~~	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: - High Impact BCS - Medium Impact BCS with ERC - SCI ~~hosting High Impact BCS or their associated EACMS or PCA~~identified independently supporting a High Impact BCS; or - SCI identified independently supporting a~~with ERC hosting~~ Medium Impact BCS with ERC~~or their associated EACMS or PCA~~ Locally mounted hardware or devices at the Physical Security Perimeter associated with: - High Impact BCS - Medium Impact BCS with ERC - SCI ~~hosting~~ identified independently supporting a High Impact BCS~~ or their associated EACMS or PCA~~; or - SCI identified independently supporting a ~~with ERC hosting~~ Medium Impact BCS with ERC ~~or their associated EACMS or PCA~~ ~~SCI hosting PACS associated with High Impact BCS~~ ~~SCI hosting PACS associated with Medium Impact BCS with ERC~~	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Requirement R1 Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Requirement R1 Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Requirement R1 Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (Requirement R1 Part 1.4)

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical Security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (Requirement R1 Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel. (Requirement R1 Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (Requirement Part 1.8) OR The Responsible Entity does not have a process

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				to retain physical access logs for 90 calendar days. (Requirement R1 Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Requirement R2 Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Requirement R2 Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (Requirement R2 Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or	The Responsible Entity did not document or implement a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (Requirement R3 Part 3.1) OR

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Requirement R3 Part 3.1)	hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Requirement R3 Part 3.1)	devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Requirement R3 Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (Requirement R3 Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	

Version	Date	Action	Change Tracking
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes and CEC language added	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	August 29–October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 **Balancing Authority**

4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 **Generator Operator**

4.1.4 **Generator Owner**

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modification to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above.	Enable only network accessible Internet Protocol (IP) ports (or services if unable to determine ports) determined to be needed by the Responsible Entity, including port ranges where needed to handle dynamic ports, per system capability. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible IP ports or services, individually or by group. • Listings of the listening ports, individually or by group, from either configuration files, command output (such as netstat), or network scans of open ports; or • Configuration of host-based firewalls, policy, or other mechanisms that only allow needed IP ports or services and deny all others.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: 1. PCA; and 2. Non-programmable communications components located inside both a PSP and ESP. Medium Impact BCS at Control Centers and their associated: 1. PCA; and 2. Non-programmable communications components located inside both a PSP and ESP. SCI identified independently supporting an Applicable System above	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI identified independently supporting: • High Impact BCS and their associated: 1. EACMS 2. PACS; and 3. PCA • Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prevent the sharing of the CPU and memory of Management Interfaces of SCI with non-CIP Systems.	Examples of evidence may include, but is not limited to, documentation of the configuration showing that the CPU and memory cannot be shared with non-CIP Systems.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above.	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for systems that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Protection [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, white-listing, privileged introspection, etc.).

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an applicable system above	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BCS is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, at a minimum, each of the following types of events, per system capability: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.
5.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems,	An example of evidence may include, but is not limited to, a listing of accounts by account types showing

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
	3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	by location, or by system type(s).	the enabled or generic account types in use.
5.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Change known default passwords, per system capability.	Examples of evidence may include, but are not limited to: - Records of a procedure that passwords are changed when new devices are in production; or - Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique.
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable System; and 5.5.2 Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: - System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account lockout parameters; or Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity has implemented and documented processes for system hardening but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Requirement R1 Part 1.2) OR The Responsible Entity has implemented and documented processes for system hardening, but has not prevented the sharing of the CPU and memory of Management Interfaces of SCI with non-CIP Systems. (Requirement R1 Part 1.4)	The Responsible Entity has implemented and documented processes for determining necessary system hardening, but had one or more unneeded network accessible services enabled. (Requirement R1 Part 1.1) OR The Responsible Entity has implemented and documented processes for determining necessary system hardening, but had one or more unneeded services enabled. (Requirement R1 Part 1.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)
R2	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	tracking or evaluating cyber security patches for applicable systems. (Requirement R2 Part 2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65	installing cyber security patches for Applicable Systems. (Requirement R2 Part 2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by	Table R2. (Requirement R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable systems. (Requirement R2 Part 2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		calendar days of the evaluation completion. (Requirement R2 Part 2.3)	applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	delegate. (Requirement R2 Part 2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (Requirement R2 Part 2.4)
R3	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Requirement R3 Part 3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (Requirement R3 Part 3.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R3. (Requirement R3). OR

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Requirement R3 Part 3.3).	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (Requirement R3 Part 3.1)
R4	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (Requirement R4 Part 4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (Requirement R4 Part 4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (Requirement R4 Part 4.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R4. (Requirement R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (Requirement R4 Part 4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (Requirement R4 Part 4.4)	capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Requirement R4 Part 4.1)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Requirement R5 Part 5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Requirement R5 Part 5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (Requirement R5 Part 5.3) OR The Responsible Entity has implemented one or more	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R5. (Requirement R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more documented process(es) for System

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more	Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords. (Requirement R5 Part 5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Requirement R5 Part 5.6)	authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See Project 2016-02 Virtualization Implementation Plan.
- See Technical Rationale for CIP-007-7

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to

Version	Date	Action	Change Tracking
			use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	TBD	Virtualization modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~initial~~ second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
~~45~~60-day formal comment period with ballot	January 21–~~February 8~~March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~May 11–June 24, 2021~~
45-day formal comment period with ballot	August ~~3~~29–~~September 16~~October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber S~~s~~ystems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber S~~s~~ystems associated with communication links ~~logically isolated from, but not providing logical isolation for, BCS or~~

~~Shared Cyber Infrastructure (SCI)~~between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber ~~s~~Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that~~Cyber Assets, Virtual Cyber Assets, or SCI performing logical isolation that~~ extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002~~-5.1~~ identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~ part applies. ~~This concept was adapted from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.~~

5. Effective Dates:

See "Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1–System Hardening

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above.	Enable only ~~logical~~ network accessible Internet Protocol (IP) ports (or services if unable to determine ports) ~~that have been~~ determined to be needed by the Responsible Entity, ~~(or logical network accessible ports if unable to determine service,~~ including port ranges where needed to handle dynamic ports~~)~~, per system capability. If a device has no provision for disabling or restricting ~~network accessible services (or~~ logical ports~~)~~ on the device~~,~~ then those ~~services (or logical~~ ports~~),~~ that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible IP ports or services, individually or by group. • Listings of the listening ports, individually or by group, from either configuration files, command output (such as netstat), or network scans of open ports; or • Configuration of host-based firewalls, policy, or other mechanisms that only allow needed IP ports or services and deny all others.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: 1. PCA~~.~~; and ~~1.~~2. Non-programmable communications components located inside both a PSP and ESP. Medium Impact BCS at Control Centers and their associated: 1. ~~-~~PCA; and ~~1.~~2. Non-programmable communications components located inside both a PSP and ESP. SCI identified independently supporting an Applicable System above ~~SCI at Control Centers hosting High or Medium Impact BCS or their associated PCA~~ ~~Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA~~ ~~Non-programmable communications components within a PSP that are not logically isolated from High or Medium impact BCS at Control Centers~~	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~1.3~~	~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~PACS;~~ ~~EACMS; or~~ ~~PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ ~~PACS;~~ ~~EACMS; or~~ ~~PCA~~	~~Enable only services that have been determined to be needed by the Responsible Entity, per system capability.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• Documentation of implemented hardening guidelines~~ ~~• Configuration management reporting~~ ~~that demonstrates the need for all enabled services.~~
1.43~~.~~	SCI identified independently supporting: • High Impact BCS and their associated: 1. EACMS 2. PACS; and 3. PCA • Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prevent the sharing of the CPU and memory of Management Interfaces of SCI with non-CIP Systems.	Examples of evidence may include, but is not limited to, documentation of the configuration showing that the CPU and memory cannot be shared with non-CIP Systems.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above. ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~- PACS;~~ ~~- EACMS; or~~ ~~- PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ ~~- PACS;~~ ~~- EACMS; or~~ - ~~PCA~~	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for systems that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ • ~~PACS;~~ • ~~EACMS; or~~ • ~~PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ • ~~PACS;~~ • ~~EACMS; or~~ • ~~PCA~~ •	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

2.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~ -	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: - Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or - A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-7 Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.4	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Protection [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ • ~~PACS;~~ • ~~EACMS; or~~ • ~~PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ • ~~PACS;~~ • ~~EACMS; or~~ • ~~PCA~~	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, white-listing, privileged introspection, etc.).

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ ~~• PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ • ~~PCA~~	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an applicable system above ~~SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include~~s~~, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BCS is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

4.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI with ERC hosting High Impact BCS or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~ ~~Management Modules with ERC of SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS~~ - ~~EACMS; or~~ - ~~PCA~~	Generate alerts for security events that the Responsible Entity determines necessitates an alert~~,~~ that includes, at a minimum, each of the following types of events, per system capability: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

4.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI at Control Centers hosting High Impact BCS, Medium Impact BCS, or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~ ~~Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS or their associated:~~ - ~~EACMS; or~~ - ~~PCA~~ ~~Management Modules of SCI hosting High BCS or their associated:~~ - ~~EACMS; or~~ - ~~PCA~~	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS, or their associated:~~ ~~• PACS;~~	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Controls

Part	Applicable Systems	Requirements	Measures
	- ~~EACMS; or~~ - ~~PCA~~ ~~Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated:~~ ~~PACS;~~ ~~EACMS; or~~ ~~PCA~~		
5.2	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS- and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use.

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ ~~PCA~~		

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI with ERC hosting High Impact BCS, Medium Impact BCS, or their associated:~~ • ~~PACS;~~ • ~~EACMS; or~~ • ~~PCA~~ ~~Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS, or their associated~~ • ~~PACS;~~ • ~~EACMS; or~~ • ~~PCA~~	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ ~~• PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ • ~~PCA~~	Change known default passwords, per system capability.	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ ~~• PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ • ~~PCA~~	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable ~~s~~System; and 5.5.2 Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable ~~s~~System.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI with ERC hosting High Impact BCS, Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ ~~• PCA~~ ~~Management Modules with ERC of SCI hosting High Impact BCS, Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ ~~• PCA~~	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

	•		

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI at Control Centers with ERC hosting High Impact BCS, Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ ~~• PCA~~ ~~Management Modules of SCI at Control Centers hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

	~~• EACMS; or~~ • ~~PCA~~		

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity has implemented and documented processes for s~~S~~ystem h~~H~~ardening but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Requirement R1 Part 1.2) OR The Responsible Entity has implemented and documented processes for system hardening, but has not prevented the sharing of the CPU and memory of Management Interfaces of SCI with non-CIP Systems. (Requirement R1 Part 1.4)	The Responsible Entity has implemented and documented processes for determining necessary s~~S~~ystem ~~H~~hardening, but had one or more unneeded network accessible services enabled. (Requirement R1 Part 1.1) OR The Responsible Entity has implemented and documented processes for determining necessary ~~S~~system ~~H~~hardening, but had one or more unneeded services enabled. (Requirement R1 Part 1.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)
R2	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not	The Responsible Entity did not implement or document one or more process(es) that included the applicable

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation	identification of sources, for tracking or evaluating cyber security patches for applicable systems. (Requirement R2 Part 2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50	include any processes for installing cyber security patches for ~~a~~Applicable ~~s~~Systems. (Requirement R2 Part 2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Requirement R2 Part 2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the	items in CIP-007-7 Table R2. (Requirement R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable systems. (Requirement R2 Part 2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	completion. (Requirement R2 Part 2.3)	calendar days but less than 65 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	CIP Senior Manager or delegate. (Requirement R2 Part 2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan. (Requirement R2 Part 2.4)
R3	N/A	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Requirement R3 Part 3.3)	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code. (Requirement R3 Part 3.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R3. (Requirement R3). OR

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Requirement R3 Part 3.3).	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code. (Requirement R3 Part 3.1)
R4	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review. (Requirement R4 Part 4.4)	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review. (Requirement R4 Part 4.4)	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2. (Requirement R4 Part 4.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R4. (Requirement R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-007-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td>The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (-except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days. (Requirement R4 Part 4.3)
OR
The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals. (Requirement R4 Part 4.4)</td><td>capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Requirement R4 Part 4.1)</td></tr>
</table>

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Requirement R5 Part 5.6)	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Requirement R5 Part 5.6)	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Requirement R5 Part 5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts. (Requirement R5 Part 5.3) OR The Responsible Entity has implemented one or more	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R5. (Requirement R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more documented process(es) for System

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more	Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access. (Requirement R5 Part 5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords. (Requirement R5 Part 5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Requirement R5 Part 5.6)	authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Requirement R5 Part 5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (5.6)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. (5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See Project 2016-02 Virtualization Implementation Plan.
- See Technical Rationale for CIP-007-7

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	

Version	Date	Action	Change Tracking
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	TBD	Virtualization modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	August 29– October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BCS) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column including justification for attempt determination criteria and documented processes for notification.
1.3	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS and their associated: • EACMS Medium ImpactBCS and their associated: • EACMS SCI identified independently supporting an Applicable System above	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations-based exercises.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact BCS and their associated: - EACMS Medium Impact BCS and their associated: - EACMS SCI identified independently supporting an Applicable System above	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact BCS and their associated: - EACMS Medium Impact BCS and their associated: - EACMS SCI identified independently supporting an Applicable System above	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA)CISA, or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and CISA.

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BCS and their associated: - EACMS Medium Impact BCS and their associated: - EACMS SCI identified independently supporting an Applicable System above	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: - One hour after the determination of a Reportable Cyber Security Incident. - By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and CISA.
4.3	High Impact BCS and their associated: - EACMS Medium Impact BCS and their associated: - EACMS SCI identified independently supporting an Applicable System above	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and CISA.

C. Compliance

1. Compliance Monitoring Process:

1.1. **Compliance Enforcement Authority:** The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Processes:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Requirement R1 Part 1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (Requirement R1 Part 1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Requirement R1 Part 1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (Requirement R1 Part 1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (Requirement R1 Part 1.2)	from Part 1.2.1, a system identified in the "Applicable Systems" column for Part 1.2. (Requirement R1 Part 1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months, not exceeding 16 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 17 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 18 calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.2 occurs. (Requirement R2 Part 2.2)	calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.3. (Requirement R2 Part 2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security	The Responsible Entity has not updated the Cyber Security Incident response plan based on any	The Responsible Entity has neither documented lessons learned nor documented the	The Responsible Entity has neither documented lessons learned nor documented the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3)	documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3) OR	absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the Cyber Security	absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and CISA, or their	The Responsible Entity failed to notify E-ISAC or CISA, or their	The Responsible Entity notified E-ISAC and CISA, or their	The Responsible Entity failed to notify E-ISAC and CISA, or their

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity notified E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to report on	successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column. (Requirement R4 Part R4)	successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity failed to notify E-ISAC or CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Requirement R4 Part 4.3) OR The Responsible Entity notified E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1.			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Requirement R4 Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Virtualization Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	

Version	Date	Action	Change Tracking
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~final~~ second draft of the proposed standard~~ being posted for a 5-day final ballot period~~.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
~~45~~60-day formal comment period with ballot	January 21–~~February 8~~March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~May 11–June 24, 2021~~
45-day formal comment period with ballot	August ~~3~~29– October 11~~September 16~~, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Remedial Action Scheme where the Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-7:

4.2.3.1 Cyber ~~s~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~s~~Systems associated with communication links ~~logically isolated from, but not providing logical isolation for, BES Cyber~~

~~Systems or SCI~~between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber ~~S~~systems, associated with communication links, between the Cyber ~~Assets~~Systems providing confidentiality and integrity of an ESP ~~, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation~~ that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BCS) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~ part applies. ~~This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.~~

5. Effective Dates:

See “Project 2016-02 ~~Virtualization~~ Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*.

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~EACMS~~	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.2	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~EACMS.~~	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the “Applicable Systems” column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column including justification for attempt determination criteria and documented processes for notification.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BCS and their associated: - EACMS Medium Impact BCS and their associated: - EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~EACMS~~	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BCS and their associated: - EACMS Medium ImpactBCS and their associated: - EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~EACMS~~	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~EACMS~~	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations-based exercises.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.2	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~EACMS~~	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the “Applicable Systems” column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~EACMS~~	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the “Applicable Systems” column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: - EACMS Medium Impact BCS and their associated: - EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~EACMS~~	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: - EACMS Medium Impact BCS and their associated: - EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~- EACMS~~	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA)~~National Cybersecurity and Communications Integration Center (NCCIC~~CISA~~)~~, ~~[1]~~ or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the “Applicable Systems” column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column according to the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

~~[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).~~

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	Applicable Systems	Requirements	Measures
4.1	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~EACMS~~	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and ~~NCCIC~~CISA.

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	Applicable Systems	Requirements	Measures
4.2	High Impact BCS and their associated: - EACMS Medium Impact BCS and their associated: - EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~EACMS~~	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: - One hour after the determination of a Reportable Cyber Security Incident. - By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable Systems" column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ~~NCCIC~~CISA.

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BCS and their associated: • EACMS Medium Impact BCS and their associated: • EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~EACMS~~	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and ~~NCCIC~~CISA.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Requirement R1 Part 1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (Requirement R1 Part 1.4) OR	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Requirement R1 Part 1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (Requirement R1 Part 1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes that include criteria to evaluate and define attempts to compromise. (Requirement R1 Part 1.2)	from Part 1.2.1, a system identified in the “Applicable Systems” column for Part 1.2. (Requirement R1 Part 1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months, not exceeding 16 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 17 calendar months between tests of the plan(s). (Requirement R2 Part 2.1)	calendar months, not exceeding 18 calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.2 occurs. (Requirement R2 Part 2.2)	calendar months between tests of the plan(s). (Requirement R2 Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the "Applicable Systems" column for Part 2.3. (Requirement R2 Part 2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security	The Responsible Entity has not updated the Cyber Security Incident response plan based on any	The Responsible Entity has neither documented lessons learned nor documented the	The Responsible Entity has neither documented lessons learned nor documented the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3)	documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.3) OR	absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the Cyber Security	absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Requirement R3 Part 3.1.1)

R #	**Time Horizon**	**VRF**	**Violation Severity Levels (CIP-008-7)**			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	
R4	**Operations Assessment**	**Lower**	The Responsible Entity notified E-ISAC and ~~NCCIC~~CISA, or their	The Responsible Entity failed to notify E-ISAC or ~~NCCIC~~CISA, or their	The Responsible Entity notified E-ISAC and ~~NCCIC~~CISA, or their	The Responsible Entity failed to notify E-ISAC and ~~NCCIC~~CISA, or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity notified E-ISAC and ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3	successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column. (Requirement R4 Part R4)	successors, of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Requirement R4 Part 4.2) OR The Responsible Entity failed to notify E-ISAC or ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	their successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but failed to report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Requirement R4 Part 4.3) OR The Responsible Entity notified E-ISAC and ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to report on one or more of the attributes after determination pursuant to Part 4.1.			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Requirement R4 Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Virtualization Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	

Version	Date	Action	Change Tracking
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. **Balancing Authority**

   4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. **Generator Operator**

   4.1.4. **Generator Owner**

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-009-7:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002-7 identification and categorization processes.

4.3. **"Applicable Systems" Columns in Tables:** Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See "Project 2016-02 Modification to CIP Standards Implementation Plan"

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above	One or more processes for the backup and storage of information required to recover applicable system functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover applicable system functionality.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BBCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS SCI identified independently supporting an Applicable System above	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS SCI identified independently supporting an Applicable System above	Test a representative sample of information used to recover applicable system functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover applicable system functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BCS SCI identified independently supporting an Applicable System above	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: 1. PACS: and 2. EACMS SCI identified independently supporting an Applicable System above	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BSC at Control Centers and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. **Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for applicable systems. OR The Responsible Entity has created recovery plan(s) for applicable systems, but the plan(s) does not address the conditions for activation in Requirement R1 Part 1.1. OR The Responsible Entity has created recovery plan(s) for applicable systems, but the plan(s) does not address three or more of the requirements in Parts Requirement R11.2 through 1.5.
R2.	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (Requirement R2 Part 2.1)	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of Applicable System functionality according to R2 Part 2.2 within 18

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Requirement R2 Part 2.3)	used in the recovery of applicable system functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Requirement R2 Part 2.3)	The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Requirement R2 Part 2.3)	calendar months between tests. (Requirement R2 Part 2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (Requirement R2 Part 2.3)

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Modification to CIP Standards Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	

Version	Date	Action	Change Tracking
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~initial~~ second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
~~45~~60-day formal comment period with ballot	January 21–~~February 8~~March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	May 11–June 24, 2021
45-day formal comment period with ballot	August 3–September 16, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-009-7:

4.2.3.1. Cyber S~~s~~ystems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber S~~s~~ystems associated with communication links ~~logically isolated from, but not providing logical isolation for, BES Cyber~~

~~Systems or Shared Cyber Infrastructure (SCI)~~between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber ~~S~~systems, associated with communication links, between the Cyber ~~Assets~~Systems~~, Virtual Cyber Assets, or SCI performing logical isolation that~~ providing confidentiality and integrity of an ESP that ~~-~~extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002-7 identification and categorization processes.

4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~ part applies. ~~This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.~~

5. **Effective Dates:** See “Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan”

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS; or~~ - ~~EACMS~~	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS; or~~ • ~~EACMS~~	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS; or~~ • ~~EACMS~~	One or more processes for the backup and storage of information required to recover applicable system functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover applicable system functionality.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact- BCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS at Control Centers or their associated:~~ • ~~PACS; or~~ • ~~EACMS~~	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS; or~~ • ~~EACMS~~	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BBCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS SCI identified independently supporting an Applicable System above	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: 1. PACS; and 2. EACMS SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS SCI identified independently supporting an Applicable System above	Test a representative sample of information used to recover applicable system functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover applicable system functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BCS SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS~~	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BCS at Control Centers and their associated: 1. PACS: and 2. EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS at Control Centers or their associated:~~ - ~~PACS; or~~ - ~~EACMS~~	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BCS and their associated: 1. PACS; and 2. EACMS Medium Impact BSC at Control Centers and their associated: 1. PACS; and 2. EACMS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS at Control Centers or their associated:~~ ~~PACS; or~~ ~~EACMS~~	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact ~~-~~the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for applicable systems. OR The Responsible Entity has created recovery plan(s) for applicable systems, but the plan(s) does not address the conditions for activation in Requirement R1 Part 1.1. OR The Responsible Entity has created recovery plan(s) for applicable systems, but the plan(s) does not address three or more of the requirements in Parts Requirement R11.2 through 1.5.
R2.	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (Requirement R2 Part 2.1)	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (Requirement R2 Part 2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of ~~a~~Applicable ~~s~~System functionality according to R2 Part 2.2 within 18

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-009-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>OR
The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Requirement R2 Part 2.2)
OR
The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Requirement R2 Part 2.3)</td><td>used in the recovery of applicable system functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Requirement R2 Part 2.2)
OR
The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Requirement R2 Part 2.3)</td><td>The Responsible Entity has not tested a representative sample of the information used in the recovery of applicable system functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Requirement R2 Part 2.2)
OR
The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Requirement R2 Part 2.3)</td><td>calendar months between tests. (Requirement R2 Part 2.2)
OR
The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (Requirement R2 Part 2.3)</td></tr>
</table>

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Requirement R3 Part 3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days -of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Requirement R3 Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See "Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan."

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	

Version	Date	Action	Change Tracking
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	August 29–October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security —Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See "Project 2016-02 Modification to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented change management process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 –Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 –Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems (BCS) and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Authorize changes to: 1.1.1. Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems; or firmware; 1.1.2. Commercially available or open-source application software, including application containers ; 1.1.3. Custom software installed, including-applications containers; and 1.1.4. Any logical network accessible ports (or services if unable to determine ports).	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change. • Documentation of authorization for cyber security patch implementation.
1.2	SCI identified independently supporting an Applicable System from Part 1.1.	Authorize changes to SCI configuration that:	Examples of evidence may include, but are not limited to:

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		1.2.1. Controls sharing of CPU or memory between systems with different impact ratings, including non-CIP Systems, hosted on SCI; and 1.2.2. Enforces an ESP between systems with different impact ratings, including non-CIP Systems, hosted on SCI.	• Documentation of authorization for changes to configuration of host affinity control between systems with different impact ratings; • Documentation of authorization for changes to policies or configurations for an ESP between systems with different impact ratings.
1.3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	For each change to the items listed in Part 1.1: 1.3.1. Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.3.2. Following the change, verify that required cyber security controls determined in 1.3.1 are not adversely affected; and 1.3.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.
1.4	High Impact BCS SCI identified independently supporting an Applicable System above	For each change to the items listed in Part 1.1 or Part 1.2, per system capability:	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		1.4.1. Prior to implementing any change in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.4.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.
1.5	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS and their associated:	Prior to a change associated with Parts 1.1.1 and 1.1.2 and when the method to do so is available to the Responsible Entity from the software source: 1.5.1. Verify the identity of the	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.5: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	software source; and 1.5.2. Verify the integrity of the software obtained from the software source.	change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Change Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Change Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Change Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Monitor at least once every 35 calendar days for unauthorized changes to the items listed in Requirement R1, Part 1.1. and Part 1.2. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems SCI identified independently supporting an Applicable System above	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of any tools used to perform the assessment, or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to: • Reports or logs from SCI mechanisms and remediation of VCAs at instantiation; or • Documention listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1, except for use on low impact BCS or SCI supporting only low impact BCS(s). *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCAs and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCAs or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCAs or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority:** “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a change authorization process(es) that includes only four or more of the required items listed in 1.1.1 through 1.1.4. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a change authorization process(es) that includes only three of the required items listed in 1.1.1 through 1.1.4. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a change authorization process(es) that includes only two of the required items listed in 1.1.1 through 1.1.4. (Requirement R1 Part 1.1) OR The Responsible Entity has documented and implemented a change authorization process(es) that includes only one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2) OR The Responsible Entity has a process as specified in Part 1.5 to verify the identity of the software source (1.5.1) but does not have a process as specified in Part 1.5 to verify the integrity of the software provided by the	The Responsible Entity has not documented or implemented any change authorization process(es). (Requirement R1) OR The Responsible Entity has documented and implemented a change authorization process(es) that includes only one of the required items listed in 1.1.1 through 1.1.4. (Requirement R1 Part 1.1) OR The Responsible Entity does not have a change authorization process(es) that requires authorization of changes to items listed in 1.1.1-1.1.4. (Requirement R1 Part 1.1) OR The Responsible Entity does not have a change

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.5.2)	authorization process(es) that requires authorization of changes to items listed in 1.2.1 to 1.2.2 (Requirement R1 Part 1.2) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing configuration. (Requirement R1 Part 1.3.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing configuration but did not verify and document that the required controls were not adversely affected following the

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				change. (Requirement R1 Part 1.3.2 & Part 1.3.3) OR The Responsible Entity does not have a process for testing changes prior to implementing a change tothe configuration. (Requirement R1 Part 1.4.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (Requirement R1 Part 1.4.2) OR The Responsible Entity does not have a process as specified in Part 1.5 to verify the identity of the software source and the integrity of the software provided by the software source when

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.5)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the items described in Requirement R1, Part 1.1. at least once every 35 calendar days. (Requirement R2 Part 2.1) OR The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the items described in Requirement R1, Part 1.2. at least once every 35

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar days. (Requirement R2 Part 2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its Applicable Systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its	The Responsible Entity has not implemented any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Applicable Systems. (Requirement R3 Part 3.2)	Applicable Systems. (Requirement R3 Part 3.2)	Applicable Systems. (Requirement R3 Part 3.2)	an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable systems.(Requirement R3 Part 3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its Applicable Systems, but did not perform the active vulnerability assessment of a Cyber System prior to it becoming an Applicable System. (Requirement R3 Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Requirement R3 Part 3.4)
R4.	The Responsible Entity documented its plan(s) for TCAs and Removable Media, but failed to manage its TCA(s) according to CIP-010-5, Requirement R4, Attachment 1, Section 1.1. (Requirement R4 Part R4) OR The Responsible Entity documented its plan(s) for TCAs and Removable Media, but failed to document the Removable Media sections according to CIP-010-5, Requirement R4,	The Responsible Entity documented its plan(s) for TCAs and Removable Media, but failed to implement the Removable Media sections according to CIP-010-5, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for TCAs and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or	The Responsible Entity documented its plan(s) for TCAs and Removable Media, but failed to authorize its TCA(s) according to CIP-010-5, Requirement R4, Attachment 1, Section 1.2. (Requirement R4) OR The Responsible Entity documented its plan(s) for TCAs and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of	The Responsible Entity failed to document or implement one or more plan(s) for TCAs and Removable Media according to CIP-010-5, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for TCAs and Removable Media, but failed to document authorization for TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Section 1.2. (Requirement R4)	mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for TCAs and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	unauthorized use for TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for TCAs and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modification to CIP Standards Implementation Plan.”.
- CIP-010-5 Technical Rationale

CIP-010-5 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets (TCA)and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCAs, individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCAs, each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCAs:

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCAs Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCAs. This can be included as part of the TCA plan(s), part of the documentation related to authorization of TCAs managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCAs managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, controls to maintain the known good state of the OS and all software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with controls to maintain the known good state of the OS and all software. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, controls to maintain the known good state of the OS and all software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCAs managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, controls to maintain the known good state of the OS and all software by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCAs managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/18	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	

Version	Date	Action	Change Tracking
4	TBD	Modified to address directives in FERC Order No. 850.	
5	TBD	Virtualization modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~final~~ second draft of the proposed standard~~ for formal 10-day comment period~~.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
~~45~~60-day formal comment period with ballot	January 21–~~February~~ March 22~~8~~, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~May 11–June 24, 2021~~
45-day formal comment period with ballot	August ~~3~~29–~~September 16~~October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. Title: Cyber Security —Change Management and Vulnerability Assessments

2. Number: CIP-010-5

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber ~~s~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~s~~Systems associated with communication links ~~logically isolated from, but not providing logical isolation for, BES Cyber~~

~~Systems or SCI~~between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber ~~s~~Systems, associated with communication links, ~~-~~between Cyber ~~Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure performing logical isolation that~~Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~ part applies. ~~This concept was adapted from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.~~

5. **Effective Date:** See “Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented change management process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 –Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 –Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems (BCS) and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~	Authorize changes to: 1.1.1. Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems; or firmware; 1.1.2. Commercially available or open-source application software, including application containers ~~Self-Contained Applications~~; 1.1.3. Custom software installed, including~~- Self-Contained A~~applications containers; and 1.1.4. Any logical network accessible ~~services,~~ports (or ~~logical ports~~services if unable to determine ~~service)~~ports).~~;~~ ~~Security patches applied;~~	Examples of evidence may include, but are not limited to: - A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change. - Documentation of authorization for cyber security patch implementation.

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	- ~~PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ - ~~PACS;~~ - ~~EACMS; or~~ - ~~PCA~~	~~SCI configuration that:~~ ~~Enforces electronic access control that permits only needed and controlled communication between systems with different impact ratings hosted on SCI;~~ ~~Enforces logical isolation between systems with different impact ratings hosted on SCI;~~ ~~Prevents sharing of CPU/Memory between systems with different impact ratings hosted on SCI; or~~ ~~Enables or disables SCI services.~~	
1.2	SCI identified independently supporting an Applicable System from Part 1.1.	Authorize changes to SCI configuration that: 1.2.1. Controls sharing of CPU or memory between systems with different impact ratings, including non-CIP Systems, hosted on SCI; and 1.2.2. Enforces an ESP between systems with different impact ratings, including non-CIP Systems, hosted on SCI.	Examples of evidence may include, but are not limited to: - Documentation of authorization for changes to configuration of host affinity control between systems with different impact ratings; - Documentation of authorization for changes to policies or configurations for an ESP between systems with different impact ratings.

CIP-010-5 Table R1 – Change Management

Part	Applicable Systems	Requirements	Measures
1.~~2~~3	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~PACS;~~ ~~EACMS; or~~ ~~PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ ~~PACS;~~ ~~EACMS; or~~	For each change to the items listed in Part 1.1: 1.~~2~~3.1. Prior to the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.~~2~~3.2. Following the change, verify that required cyber security controls determined in 1.~~2~~3.1 are not adversely affected; and 1.~~2~~3.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-5 Table R1 – Change Management

Part	Applicable Systems	Requirements	Measures
	~~• PCA~~		
1.~~3~~4	High Impact BCS SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS~~	For each change to the items listed in Part 1.1 or Part 1.2, per system capability: 1.~~3~~4.1. Prior to implementing any change in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.~~3~~4.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		production environments.	
1.45	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS and their associated EACMS and PACS.~~ ~~Management Modules of SCI hosting High or Medium Impact BCS and their associated EACMS and PACS.~~ Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.45: (1) the actual terms and conditions of a procurement contract; and (2) vendor	Prior to a change associated with ~~Requirement~~ Parts 1.1.1~~,~~ and 1.1.2~~, and 1.1.5,~~ and when the method to do so is available to the Responsible Entity from the software source: 1.45.1. Verify the identity of the software source; and 1.45.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-5 Table R1 – Change Management			
Part	Applicable Systems	Requirements	Measures
	performance and adherence to a contract.		

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Change Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Change Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Change Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Monitor at least once every 35 calendar days for unauthorized changes to the items ~~described~~ listed in Requirement R1, Part 1.1. and Part 1.2. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ ~~• PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ • ~~PCA~~	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BCS.~~ ~~Management Modules of SCI hosting High Impact BCS.~~	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High Impact BES Cyber Systems or their associated:~~ ~~PACS;~~ ~~EACMS; or~~ ~~PCA~~ ~~Management Modules of SCI hosting High Impact BCS or their associated:~~ ~~EACMS; or~~ ~~PCA~~	Prior to becoming a new Applicable System, ~~P~~perform an active vulnerability assessment of the new Applicable System, ~~prior to logically connecting an additional applicable Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure to a production environment, per system capability,~~ except for: • ~~for CIP Exceptional Circumstances,~~like replacements of the same type of Cyber System with a ~~or deployments using a previously assessed~~ configuration of the previous or other existing Cyber System; or • CIP Exceptional Circumstances. ~~. The production environment does not include devices being actively remediated and logically isolated.~~	An example of evidence may include, but is not limited to:~~,~~ • The output of any tools used to perform the assessment, or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System ~~BES Cyber System or SCI~~. ~~a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure) and the output of any tools or Management Systems used to perform the assessment.~~

CIP-010-5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.4	High Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above ~~SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ ~~• PCA~~ ~~Management Modules of SCI hosting High or Medium Impact BCS or their associated:~~ ~~• PACS;~~ ~~• EACMS; or~~ ~~PCA~~	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to:~~,~~ • ~~a r~~Reports or logs from SCI mechanisms and remediation of VCAs at instantiation; or ~~of Management System actions, or a~~ • ~~d~~Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity~~, for its high impact and medium impact BES Cyber Systems and associated SCI and Protected Cyber Assets,~~ shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1, ~~that~~ except for use on low impact BCS or SCI supporting only low impact BCS(s)~~include the sections in Attachment 1~~. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for ~~Transient Cyber Asset~~TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for ~~Transient Cyber Asset~~TCAs and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use ~~Transient Cyber Asset(~~TCAs~~)~~ or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use ~~Transient Cyber Asset(~~TCAs~~)~~ or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a change ~~management~~ authorization process(es) that includes only four or more of the required items listed in 1.1.1 through 1.1.4~~6~~. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a change ~~management~~ authorization process(es) that includes only three of the required items listed in 1.1.1 through 1.1.4~~6~~. (Requirement R1 Part 1.1)	The Responsible Entity has documented and implemented a change ~~management~~ authorization process(es) that includes only two of the required items listed in 1.1.1 through 1.1.4~~6~~. (Requirement R1 Part 1.1) OR The Responsible Entity has documented and implemented a change authorization process(es) that includes only one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2) OR The Responsible Entity has a process as specified in Part 1.5~~4~~ to verify the identity of the software source (1.5~~4~~.1) but does not have a process as specified in Part 1.5~~4~~ to verify the integrity of the	The Responsible Entity has not documented or implemented any change ~~management~~ authorization process(es). (Requirement R1) OR The Responsible Entity has documented and implemented a change ~~management~~ authorization process(es) that includes only one of the required items listed in 1.1.1 through 1.1.4~~6~~. (Requirement R1 Part 1.1) OR The Responsible Entity does not have a change ~~management~~ authorization process(es) that requires authorization of changes to items listed in 1.1.1-1.1.4~~6~~. (Requirement R1 Part 1.1) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.5~~4~~.2)	The Responsible Entity does not have a change authorization process(es) that requires authorization of changes to items listed in 1.2.1 to 1.2.2 (Requirement R1 Part 1.2) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing configuration. (Requirement R1 Part 1.3~~2~~.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing configuration but did not verify and

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				document that the required controls were not adversely affected following the change. (Requirement R1 Part 1.3~~2~~.2 & Part 1.3~~2~~.3) OR The Responsible Entity does not have a process for testing changes prior to implementing a change tothe configuration. (Requirement R1 Part 1.4~~3~~.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (Requirement R1 Part 1.4~~3~~.2) OR The Responsible Entity does not have a process as

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				specified in Part 1.54 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.54)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the items described in Requirement R1, Part 1.1. at least once every 35 calendar days. (Requirement R2 Part 2.1) OR The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				items described in Requirement R1, Part 1.2. at least once every 35 calendar days. (Requirement R2 Part 2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its A~~a~~pplicable S~~s~~ystems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its A~~a~~pplicable S~~s~~ystems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for A~~a~~pplicable S~~s~~ystems, but has performed an active vulnerability assessment more than 36 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its A~~a~~pplicable S~~s~~ystems, but has performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its A~~a~~pplicable S~~s~~ystems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for A~~a~~pplicable S~~s~~ystems, but has performed an active vulnerability assessment more than 39 months, but	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its A~~a~~pplicable S~~s~~ystems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its A~~a~~pplicable S~~s~~ystems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for A~~a~~pplicable S~~s~~ystems, but has performed an active vulnerability assessment more than 42 months, but	The Responsible Entity has not implemented any vulnerability assessment processes for one of its A~~a~~pplicable S~~s~~ystems. (Requirement R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its A~~a~~pplicable S~~s~~ystems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable systems. (Requirement R3 Part 3.1) OR The Responsible Entity has implemented one or more

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	less than 39 months, since the last active assessment on one of its A~~a~~pplicable S~~s~~ystems. (Requirement R3 Part 3.2)	less than 42 months, since the last active assessment on one of its A~~a~~pplicable S~~s~~ystems. (Requirement R3 Part 3.2)	less than 45 months, since the last active assessment on one of its A~~a~~pplicable S~~s~~ystems. (Requirement R3 Part 3.2)	documented active vulnerability assessment processes for A~~a~~pplicable S~~s~~ystems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable systems.(Requirement R3 Part 3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its A~~a~~pplicable S~~s~~ystems, but did not perform the active vulnerability assessment of a Cyber System prior to it becoming an~~its~~ A~~a~~pplicable S~~s~~ystem~~s~~. (Requirement R3 Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessment processes for each of its A~~a~~pplicable S~~s~~ystems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Requirement R3 Part 3.4)
R4.	The Responsible Entity documented its plan(s) for ~~Transient Cyber Asset~~TCAs and Removable Media, but failed to manage its ~~Transient Cyber Asset~~TCA(s) according to CIP-010-5, Requirement R4, Attachment 1, Section 1.1. (Requirement R4 Part R4) OR The Responsible Entity documented its plan(s) for	The Responsible Entity documented its plan(s) for ~~Transient Cyber Asset~~TCAs and Removable Media, but failed to implement the Removable Media sections according to CIP-010-5, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for	The Responsible Entity documented its plan(s) for ~~Transient Cyber Asset~~TCAs and Removable Media, but failed to authorize its ~~Transient Cyber Asset~~TCA(s) according to CIP-010-5, Requirement R4, Attachment 1, Section 1.2. (Requirement R4) OR The Responsible Entity documented its plan(s) for	The Responsible Entity failed to document or implement one or more plan(s) for ~~Transient Cyber Asset~~TCAs and Removable Media according to CIP-010-5, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Transient Cyber Asset~~TCAs and Removable Media, but failed to document the Removable Media sections according to CIP-010-5, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity documented its plan(s) for ~~Transient Cyber Asset~~TCAs and Removable Media, but failed to document authorization for ~~Transient Cyber Asset~~TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Section 1.2. (Requirement R4)	~~Transient Cyber Asset~~TCAs and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Asset~~TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for ~~Transient Cyber Asset~~TCAs and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for ~~Transient Cyber Asset~~TCAs managed by a party other than the	~~Transient Cyber Asset~~TCAs and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Asset~~TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity documented its plan(s) for ~~Transient Cyber Asset~~TCAs and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for ~~Transient Cyber Asset~~TCAs managed by a party other than the	

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
		Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See "Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan.".
- CIP-010-5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/18	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	TBD	Modified to address directives in FERC Order No. 850.	
5	TBD	Virtualization modifications	

CIP-010-5 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets (TCA)and Removable Media as required under Requirement R4.

Section 1. ~~Transient Cyber Asset~~TCA(s) Managed by the Responsible Entity.

1.1. ~~Transient Cyber Asset~~TCA Management: Responsible Entities shall manage ~~Transient Cyber Asset(~~TCAs~~)~~, individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection,~~ to a BES Cyber System~~BCS~~,~~ or (3) a combination of both (1) and (2) above.

1.2. ~~Transient Cyber Asset~~TCA Authorization: For each individual or group of ~~Transient Cyber Asset(~~TCAs~~)~~, each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset~~TCA (per ~~Transient Cyber Asset~~TCA capability):

- Security patching, including manual or managed updates;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code~~Live operating system and software executable only from read-only media~~;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;

- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of ~~Transient Cyber Asset(s)~~TCAs:

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. ~~Transient Cyber Asset(s)~~TCAs Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset~~TCA (per ~~Transient Cyber Asset~~TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of ~~O~~other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code~~use of live operating system and software executable only from read-only media~~;
- Review of system hardening used by the party; or
- Review of ~~O~~other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset~~TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code ~~to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets~~, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ~~to a BES Cyber System or Protected Cyber Assets~~; and

3.2.2. Mitigate the threat of detected malicious code ~~on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets~~.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the ~~Transient Cyber Asset(~~TCAs~~)~~. This can be included as part of the ~~Transient Cyber Asset~~TCA plan(s), part of the documentation related to authorization of ~~Transient Cyber Asset(~~TCAs~~)~~ managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of ~~Transient Cyber Asset(~~TCAs~~)~~ managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, controls to maintain the known good state of the OS and all software~~the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software~~. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with controls to maintain the known good state of the OS and all software~~system hardening practices~~. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, controls to maintain the known good state of the OS and all software~~processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code~~, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for ~~Transient Cyber Asset(~~TCAs~~)~~ managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, controls to maintain the known good state of the OS and all software ~~use of live of operating systems or system hardening performed~~ by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset(~~TCAs~~)~~ managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	August 29– October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-Y
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-Y:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. **“Applicable Systems” Columns in Tables:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

6. **Effective Dates:** See Project 2016-02 “Modification to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to “Applicable Systems” identified in *CIP-011-Y Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-Y Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-Y Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-Y Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems (BCS) and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Method(s) to identify BCSI.	Examples of evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity’s information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity’s information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity’s information protection program.

CIP-011-Y Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premises BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premises BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or

CIP-011-Y Table R1 – Information Protection Program			
Part	Applicable Systems	Requirements	Measures
			• Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-Y Table R2 –Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-Y Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-Y Table R2 –Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Method(s) to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the "Applicable Systems" column).	Examples of evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

B. Compliance

1. **Compliance Monitoring Process:**

   1.1. **Compliance Enforcement Authority:** "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

   1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
   - If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented	The Responsible Entity implemented one or more documented	The Responsible Entity has not documented or implemented any

R #	**Time Horizon**	**VRF**	**Violation Severity Levels (CIP-011-Y)**			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	processes for applicable requirement parts in CIP-011-X Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting~~Standards Committee approved Standard Authorization Request (SAR) for posting~~	March 9, 2016~~March 22, 2019~~
SAR posted for comment~~SAR posted for comment~~	March 23–April 21, 2016~~March 28, 2019 – April 26, 2019~~
SAR posted for comment~~45-day formal comment period with ballot~~	June 1–June 30, 2016~~December 20, 2019 – February 3, 2020~~
SC Accepted the SAR~~45-day formal comment period with ballot~~	July 20, 2016~~August 6–September 21, 2020~~
60-day formal comment period with ballot~~45-day formal comment period with ballot~~	January 21–March 22, 2021~~March 25 – May 10, 2021~~
45-day formal comment period with ballot~~10-day final ballot~~	June 30 – August 13, 2021~~June 2 – 11, 2021~~

Anticipated Actions	Date
45-day formal comment period with ballot	August 29– October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-~~X~~Y

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~X~~Y:

4.2.3.1 Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~ Systems associated with communication ~~networks and data communication~~ links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5.1a~~ identification and categorization processes.

5. “Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

~~5.~~6. Effective Dates: See Project 2016-02 “Modification to CIP Standards Implementation Plan”~~ for CIP-011-X~~.

6. ~~**Background:** Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *“Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].”* The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program.~~

~~The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~“Applicable Systems” Columns in Tables:~~

~~Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

~~High Impact BES Cyber Systems –~~ ~~Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.~~

~~Medium Impact BES Cyber Systems –~~ ~~Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.~~

~~**Electronic Access Control or Monitoring Systems (EACMS) –** Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS) –** Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

~~**Protected Cyber Assets (PCA) –** Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to “Applicable Systems” identified in *CIP-011-~~X~~ Y Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-~~X~~ Y Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~X~~ Y Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~X~~ Y Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems (BCS) and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Method(s) to identify BCSI.	Examples of ~~acceptable~~ evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity’s information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity’s information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity’s information protection program.

CIP-011-~~X~~Y Table R1 – Information Protection Program

Part	Applicable Systems	Requirements	Measures
1.2	High Impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System above	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premises BCSI may include, but are not limited to, the following: - Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or - Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premises BCSI may include, but are not limited to, the following: - Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or - Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or

CIP-011-~~X~~ Y Table R1 – Information Protection Program			
Part	Applicable Systems	Requirements	Measures
			- Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~X~~ Y Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~X~~ Y Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~X~~ Y Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	~~Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action~~Method(s) to prevent the unauthorized retrieval of BCSI from ~~the Cyber Asset data storage media~~Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the “Applicable Systems” column).	Examples of ~~acceptable~~ evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-~~X~~ Y Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
~~2.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~0. EACMS;~~ ~~0. PACS; and~~ ~~PCA~~	~~Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.~~	~~Examples of acceptable evidence may include, but are not limited to, the following:~~ ~~Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or~~ ~~Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.~~

B. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-Y~~X~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity documented, but did not, implement one or more BCSI protection program(s). (R1) OR The Responsible Entity documented but did not implement at least one method to identify BCSI. (1.1) OR The Responsible Entity documented but did not implement at least one method to protect and securely handle BCSI. (1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (R1)
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented	The Responsible Entity implemented one or more documented	The Responsible Entity has not documented or implemented any

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-Y~~X~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				processes but did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1)	processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BCSI from the BES Cyber Asset. (2.1~~2~~)	processes for applicable requirement parts in CIP-011-X Table R3 – BES Cyber Asset Reuse and Disposal. (R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30–August 13, 2021

Anticipated Actions	Date
45-day formal comment period with ballot	August 29–October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems and their associated cyber systems.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. **Balancing Authority**

4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.3. **Generator Operator**

4.1.4. **Generator Owner**

4.1.5. **Reliability Coordinator**

4.1.6. **Transmission Operator**

4.1.7. **Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-3:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. **Effective Date:** See “Project 2016-02 Modification to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems (BCS), their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and SCI identified independently supporting these BCS or their associated EACMS and PACS. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of systems listed in R1 to identify and assess cyber security risk(s) to the Bulk Electric System (BES) from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring systems listed in R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do not include one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do not include two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				cyber security risk management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2; OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	R1 Part 1.2.1 through Part 1.2.6.	Requirement R1 Part 1.2.1 through Part 1.2.6.		The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modification to CIP Standards Implementation Plan”

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	
3	TBD	Virtualization conforming changes.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~initial~~ second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
~~45~~60-day formal comment period with ballot	January 21–~~February~~ March 22~~8~~, 2021
45-day formal comment period with ballot	June 30–August 13, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~May 11–June 24, 2021~~
45-day formal comment period with ballot	August ~~3~~29–~~September 16~~October 11, 2021
Final Ballot	October 19–28, 2021
Board adoption	November 4, 2021

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems and their associated cyber systems.

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.3. Generator Operator

    4.1.4. Generator Owner

    4.1.5. Reliability Coordinator

    4.1.6. Transmission Operator

    4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-3:

4.2.3.1. Cyber ~~s~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~s~~Systems associated with communication links ~~logically isolated from, but not providing logical isolation for, BES Cyber Systems (BCS) or Shared Cyber Infrastructure (SCI)~~between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber ~~s~~Systems, associated with communication links, between Cyber ~~Assets~~Systems~~, Virtual Cyber Assets, or SCI performing~~

~~logical isolation that~~ providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. **Effective Date:** See "Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems (BCS), their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and ~~the~~ SCI identified independently supporting these BCS or their associated EACMS and PACS. ~~hosting high or medium impact BCS or their associated Electronic Access Controlling or Monitoring System (EACMS) or Physical Access Control System (PACS).~~ The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of systems listed in R1 ~~of SCI, BCS, and their associated EACMS and PACS~~ to identify and assess cyber security risk(s) to the Bulk Electric System (BES) from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring systems listed in R1 ~~SCI, BCS, and their associated EACMS and PACS,~~ that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor ~~for use in the SCI, BCS and their associated EACMS and PACS~~; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the

scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

“Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do not include one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do not include two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				cyber security risk management plan(s) as specified in the Requirement.
R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2; OR

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>R1 Part 1.2.1 through Part 1.2.6.</td><td>Requirement R1 Part 1.2.1 through Part 1.2.6.</td><td></td><td>The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.</td></tr>
<tr><td>R3.</td><td>The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.</td><td>The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.</td><td>The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.</td><td>The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.</td></tr>
</table>

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 ~~Virtualization~~ Modification to CIP Standards Implementation Plan”

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	TBD	Modified to address directive in FERC Order No. 850.	
3	TBD	Virtualization conforming changes.	

Project 2016-02 Virtualization Implementation Plan

Applicable Standard(s)

- Reliability Standard CIP-002-7 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-9 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-7 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-8 – Cyber Security – BES Cyber System Logical Isolation
- Reliability Standard CIP-006-7 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-7 – Cyber Security – System Security Management
- Reliability Standard CIP-008-7 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-5 – Cyber Security – Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-3 – Cyber Security – Information Protection
- Reliability Standard CIP-013-3 – Cyber Security – Supply Chain Risk Management
- Proposed new or modified terms listed in the “CIP Definitions Posting Document (Project 2016-02)”

These standards and Definitions of Terms used in the versions listed above of the CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

These standards and new and modified terms used in the standards above will be referenced as the “Revised CIP Standards and Definitions” within the Implementation Plan.

Requested Retirement(s)

- Reliability Standard CIP-002-6 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-8 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-6 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)
- Reliability Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-6 – Cyber Security – System Security Management

- Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-2 – Cyber Security – Information Protection
- Reliability Standard CIP-013-2 – Cyber Security – Supply Chain Risk Management
- Proposed terms for retirement listed in the "Definitions of Terms used in the above listed CIP Cyber Security Standards" document

These standards and definitions used in the versions listed above will be referenced as the "Requested CIP Retired Standards and Definitions" within the Implementation Plan.

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved or retired before the Applicable Standard become effective:

- BES Cyber Asset (BCA)
- BES Cyber System
- BES Cyber System Information
- CIP Senior Manager
- Cyber Asset
- Cyber Security Incident
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate Systems (IS)
- Management Interface
- Management Module
- Management Systems
- Physical Access Control Systems
- Physical Security Perimeter (PSP)

- Protected Cyber Asset (PCA)
- Removable Media
- Reportable Cyber Security Incident
- Self-Contained Application
- Shared Cyber Infrastructure (SCI)
- Transient Cyber Asset (TCA)
- Virtual Cyber Asset (VCA)

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions. The intent of the Compliance Dates for Early Adoption of Revised CIP Standards and Definitions section is to permit Responsible Entities the adoption to comply with the Revised CIP Standards and Definitions prior to the Effective Date.

Effective Date and Phased-in Compliance Dates

The Effective Dates for the Revised CIP Standards and Definitions are provided below. As noted in the General Considerations section above, the standard drafting team determined to clarify initial performance of periodic requirements and permit Responsible Entities to comply with the Revised CIP Standards and Definitions prior to the effective date. These provisions also are provided below.

Revised CIP Standards and Definitions

Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the

---

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the date the Revised CIP Standards and Definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards and Definitions.

Compliance Dates for Early Adoption of Revised CIP Standards and Definitions

A Responsible Entity may elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the Revised CIP Standards and Definitions. Responsible Entities must comply with applicable Requested CIP Retired Standards and Definitions until that date.

Retirement Date

Requested CIP Retired Standards and Definitions

The Requested CIP Retired Standards and Definitions shall be retired immediately prior to the effective date of the Revised CIP Standards and Definitions in the particular jurisdiction in which the Revised CIP Standards and Definitions are becoming effective.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on the **Virtualization Modifications** by **8 p.m. Eastern, Friday, August 13, 2021.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Jordan Mallory (404-446-2589).

Background Information

Project 2016-02 (1) addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and (2) considers the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for Standard Drafting Team Consideration (V5TAG Transfer Document).

The V5TAG, which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP Version 5 standards and to support industry’s implementation activities. During the V5TAG’s activities, it identified certain issues with the CIP Reliability Standards that would be better addressed by a standard drafting team (SDT) for the CIP Reliability Standards. The V5TAG developed the CIP Version 5 Transition Advisory Group Issues for Consideration document to formally recommend that the SDT address these issues and consider modifications to the standard language during the standards development process. Among other issues, the V5TAG stated “The CIP Version 5 standards comments.

Summary of Changes Overview

The SDT reviewed all comments and made modifications to the Reliability Standards and Definitions accordingly. The SDT revised many standards based on industry comments to revert much of the language back to previously approved, which will be reflected as redline, but is currently the approved language. Below are questions the SDT is seeking industry input. In order to allow the SDT to sort comments received by topic, the SDT respectfully requests comments be submitted with the respective question topic. The SDT thanks industry for your time and review during this comment period.

Questions

1. Are the two options for identification of SCI within CIP-002 clear and is it understood that when SCI is included in the CIP Systems that it is treated like the CIP System, it is a part of for CIP Requirement Applicability?

   ☐ Yes
   ☐ No

   Comments:

2. The Applicable Systems column may include “SCI identified independently…” Is this clear or is additional clarification (such as “SCI identified as supporting, but not part of…”) needed?

   ☐ Yes
   ☐ No

   Comments:

3. The SDT modified the ERC definition to reference “outside the asset containing”. This is to allow scoping based on connectivity of the logging systems as required by CIP-007 Requirement R4 as well as the scoping of requirement parts in CIP-004 and CIP-006 based on risk. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

4. The SDT proposes that the modified ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

5. The SDT modified the IRA definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

6. The SDT modified the Management Interface definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

7. As discussed in the CIP Definitions and Exemptions Technical Rationale (TR), the SDT believes that the use of configurations or policy in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

8. The SDT added new and revised several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☐ No

Comments:

9. The SDT revised CIP-002 based on industry comments. Do you agree with the proposed changes to the CIP-002 Reliability Standard? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☐ No

Comments:

10. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☐ No

Comments:

11. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☐ No

Comments:

12. The SDT revised CIP-010 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☐ No

Comments:

13. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 (conforming changes) based on industry comments. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

    ☐ Yes
    ☐ No

    Comments:

14. Please provide any additional comments for the SAR drafting team to consider, if desired.

CIP Definitions

Project 2016-02 Modifications to CIP Standards

The standard drafting team (SDT) is seeking comment on the following new, modified, or retired terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS)	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	One or more BES Cyber Assets logically grouped by a R~~r~~esponsible E~~e~~ntity to perform one or more reliability tasks for a functional entity, including Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.
BES Cyber System Information	Information about the BES Cyber System that could be used to gain	Information about the BES Cyber System or Shared Cyber

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
(BCSI)	unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	Infrastructure that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Standards~~, CIP-002 through CIP-011.~~
CIP System ***New Definition***		A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
		Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.	Programmable electronic devices, including the hardware, software, and data in those devices; excluding Shared Cyber Infrastructure.
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: • ~~–~~For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or (4) Shared Cyber Infrastructure; or • Disrupts or attempts to disrupt the operation of a BES Cyber System.
Cyber System ***New Definition***		A group of one or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Intermediate Systems and SCI grouped, by the Responsible Entity, in the EACMS it supports.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and	A policy enforcement point or a Cyber Asset interface~~on an Electronic Security Perimeter~~ that allows routable communication ~~between Cyber Assets outside an~~

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
	Cyber Assets inside an Electronic Security Perimeter.	~~Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter~~to and from the BES Cyber System within an Electronic Security Perimeter.
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to communicate to a CIP System using ~~access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via~~ a bi-directional routable protocol ~~connection~~from outside the asset containing the CIP System.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	~~The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.~~ A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.
~~**Cyber System**~~		~~A group of one or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.~~
~~**CIP System**~~		~~A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.~~
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access	User-initiated real-time access by a person from outside of the Responsible Entity's Electronic Security Perimeters (ESP)~~.~~ using a

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
	originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	routable protocol: - to a Cyber System within an ESP; - through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter; - To Management Interfaces of ~~an~~ Shared Cyber Infrastructure; or - To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforces an ESP. ~~User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.~~
Intermediate Systems	A Cyber Asset or collection of Cyber Assets performing access control to	One or more Electronic Access Control or Monitoring Systems that

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
	restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	~~is~~are used to restrict Interactive Remote Access to only authorized users.~~A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.~~
Management Interface ***New Definition***		A user interface, logical interface, or dedicated physical port that is used to: • Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or • Provide lights-out management capabilities; or • Configure an Electronic Security Perimeter; excluding physical user interfaces (e.g., power switch, touch panel, etc.).
~~Management Module~~		~~An autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.~~
~~Management Systems~~		~~Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Cyber Assets or Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring~~

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
		~~those assets and systems; excluding Management Modules.~~
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers	Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) (including SCI grouped, by the Responsible Entity, in the Physical Access Control Systems it supports) that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	One or more Cyber Assets or Virtual Cyber Assets that: • Are within an Electronic Security Perimeter but are not part of the highest impact BES Cyber System within the same Electronic Security Perimeter; or • Share CPU or memory with any part of a BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to the Electronic Security Perimeter. ~~connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the~~

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
		~~highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.~~
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, Shared Cyber Infrastructure, a network within an ESP, or a Protected Cyber Asset. ~~Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	A Cyber Security Incident that compromised or disrupted: • ~~-~~A BES Cyber System that performs one or more reliability tasks of a functional entity; • ~~-~~An Electronic Security Perimeter of a high or medium impact BES Cyber System; ~~or~~ • ~~-~~An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or • ~~-~~Shared Cyber Infrastructure supporting a BES Cyber System
~~**Self-Contained Application**~~		~~Immutable software binaries containing operating system~~

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
		~~dependencies and application software packaged to execute in an isolated environment.~~
Shared Cyber Infrastructure (SCI) ***New Definition***	One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.	One or more programmable electronic devices, including the software and Management Interfaces, that share: • CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, or PACS; or • storage resources with any part of a BES Cyber System or their associated ~~Electronic Access Control or Monitoring Systems~~EACMS or ~~Physical Access Control Systems~~PACS. Each SCI is either: • included in one or more BES Cyber Systems, EACMS, or PACS; or • identified independently. SCI does not include the supported VCA or CA with which it shares its resources. ~~(excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.~~
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code,	A Cyber Asset or Virtual Cyber Asset that is: 1. capable of transmitting or

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
	2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	transferring executable code, 2. not included in a BES Cyber System, ~~2. not a Shared Cyber Infrastructure associated with high or medium impact BES Cyber Systems~~ 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. connected for 30 consecutive calendar days or less: • to a network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or • directly ~~connected~~ (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) ~~for 30 consecutive calendar days or less~~ to a: ▪ BES Cyber Asset, ▪ Shared Cyber Infrastructure, or ▪ ~~Network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or~~ Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
		Virtual machines hosted on a physical TCA can be treated as software on that physical TCA. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Virtual Cyber Asset (VCA) ***New Definition***		A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure or a PCA.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Technical Rationale

New and Modified Terms, and Exemption Language Used in NERC Reliability Standards | Project 2016-02 Modification to CIP Standards

Proposed Modified Terms:

BES Cyber Asset (BCA)

A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Rationale

The BCA definition is changing to allow for BCA to be either Cyber Assets (hardware included) or Virtual Cyber Assets (VCA) (software only virtual machines without the underlying hardware). The definition of BCA excludes the underlying hardware for virtualized environments, now defined as Shared Cyber Infrastructure (SCI). The standards drafting team (SDT) recognizes that SCI indeed has the same impact as a virtual BCA and even more so if hosting numerous BCA, and those risks will be addressed in requirements specifically for the SCI. See the VCA and SCI definition below.

BES Cyber System (BCS)

One or more BES Cyber Assets logically grouped by a Responsible Entity to perform one or more reliability tasks for a functional entity, including Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.

Rationale

The SDT is adding the option (known as the “all-in” scenario) for entities to group their SCI within a BCS it supports. See the CIP-002 Technical Rationale document for a description of the options for identifying SCI and reasons an entity may choose between the options. In addition, to shorten several applicability statements within the body of CIP standards, the SDT proposes that “BCS” be added as the defined acronym for “BES Cyber System” to the NERC glossary.

BES Cyber System Information (BCSI)

Information about the BES Cyber System or Shared Cyber Infrastructure that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring

Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System

Rationale

Conforming changes such that BCSI includes information about SCI.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Standards.

Rationale

Remove explicit reference to the CIP standards as only “CIP-002 through CIP-011” as the body of CIP standards has grown beyond CIP-011. As an example, the CIP Senior Manager also has requirements within CIP-013.

Cyber Assets

Programmable electronic devices, including the hardware, software, and data in those devices; excluding Shared Cyber Infrastructure.

Rationale

Modified to explicitly exclude SCI from the definition of CA such that SCI and CA are two hardware ‘forms’ on which the other types of cyber systems reside. SCI is another form of ‘programmable electronic devices’ that do NOT include the software and data in the hardware devices. SCI is defined separately such that it can be the object of additional requirements based on its unique risks.

Cyber Security Incident

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System, or (4) Shared Cyber Infrastructure; or
- Disrupts or attempts to disrupt the operation of a BES Cyber System.

Rationale

Modified to add SCI to the scope of compromised or attempted compromise systems.

Electronic Access Control or Monitoring Systems (EACMS)

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or Shared Cyber Infrastructure. This includes Intermediate Systems and SCI grouped, by the Responsible Entity, in the EACMS it supports.

Rationale

Modified to add VCA and SCI as two other forms that an EACMS can take and add SCI as an object of the access control or monitoring. EACMS also includes the SCI grouped by the Responsible Entity with a virtualized EACMS it supports.

Electronic Access Point (EAP)

A policy enforcement point, or a Cyber Asset interface that allows routable communication to and from the BES Cyber System within an ESP.

Rationale

As network security moves deeper into the infrastructure, its no longer necessary to prescribe that network security be performed on a 'Cyber Asset interface on an ESP'; at one point on a network edge. Zero Trust, for example, highly distributes the network security model and is not perimeter-based. With the added flexibility in CIP-005 to adopt these models in addition to the traditional ESP model, the term EAP is being modified to allow for policy enforcement points and no longer prescribes an architecture.

External Routable Connectivity (ERC)

The ability to communicate to a CIP System using a bi-directional routable protocol from outside the asset containing the CIP System.

Rationale

The ERC definition is undergoing a clarification from an ability to "access" to an ability to "communicate" so it is a more connectivity-based term and distinguished from user access-based terms such as IRA. The ERC term is used throughout the CIP Standards within the Applicable Systems column as a scoping mechanism based on the inherent risk associated with external routable connectivity as well as to limit the scope of requirements that would require ERC to function. The SDT is maintaining this use of ERC, but also clarifying the relationship between ERC and IRA in that a non-routable, serial only CIP System may have ERC and have IRA through the ERC through a subsequent IP/serial conversion (see changes to IRA definition). The definition was also modified to use the newly proposed 'CIP System' glossary term as shorthand for the various types of Cyber Systems that are in CIP scope. The intent is a CIP System within a BES asset has ERC if it is reachable by a bi-directional routable protocol from outside of the asset containing it. Cyber Assets on an isolated, standalone routable protocol network within a BES asset that cannot be reached from outside the asset (e.g., a PLC, HMI, and switch network as a standalone system with no firewall or router connections to any other network) would not have ERC.

ERC is no longer based on 'external' being defined in terms of the ESP as ESPs are changing in light of Zero Trust models. Zero Trust will shrink ESP's over time to the smallest, most granular object possible including a single device or possibly to process or resource level on a device. In this model, many dynamic, short-lived session level 'perimeters' may exist. In these implementations as the ESP shrinks, if ERC continues to be based on ESP then the 'external' in ERC begins to lose meaning, thus the move away from ESP for the determination of what is external. Therefore, the SDT is modifying the object of the "outside of " statement to be external to the asset containing the CIP System being accessed, because that ts the logical object where both the risk elevates, and the connectivity capability must exist so that the ERC definition can fulfill both of the current scoping goals in place within the CIP Standards.

Electronic Security Perimeter (ESP)

A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Rationale

The traditional network-edge Electronic Security Perimeter remains a valid network security model, however it is no longer the only prescribed model as CIP-005 allows other access control models that are not based on network perimeters such as Zero Trust architectures. The proposed ESP definition is more objective-oriented and is no longer network-location centric as security models such as Zero Trust move away from implicit trust within network perimeters and using network location as a primary factor in access control decisions. In these models, the perimeter shrinks to increasingly more granular levels, potentially down to a process or resource level on a BCS and nothing on the network is trusted for unrestricted communications. The proposed definition allows for an ESP to be (a) static point(s) on a network boundary such as a traditional FW that is enforcing access policies or configurations (e.g., FW rulesets), (b) many dynamic, short-lived, session-level 'perimeters' established at time of access that are network independent (e.g., users to resources, for example), or (c) hybrid implementations combining elements of both.

Interactive Remote Access (IRA)

User-initiated real-time access by a person from outside of the Responsible Entity's Electronic Security Perimeters (ESP) using a routable protocol:

- to a Cyber System within an ESP;
- through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;
- To Management Interfaces of a Shared Cyber Infrastructure; or
- To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforces an ESP.

.

Rationale

The proposed IRA definition changes in two fundamental ways: (1) to incorporate as IRA situations where a BCS has ERC and through it users outside of any of the Responsible Entity's ESPs have access to non-routable (serial) CIP Systems within the asset through a subsequent IP/serial conversion, and (b) to include the Management Interfaces of SCI or EACMS that enforce an ESP as targets of IRA, such that IRA includes not only objects within an ESP, but the objects that enforce the ESP as well. The references to ownership of the remote client have been removed.

Intermediate Systems

One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users .

Rationale

The IS definition is changing to remove requirement language (i.e., where an Intermediate System must reside) embedded within the definition. Such language has been moved to CIP-005 R2 within a mandatory requirement. The definition was also updated from a Cyber Asset focus to an EACMS focus to include more forms (i.e., VCA) the Intermediate System can take.

Physical Access Control Systems (PACS)

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) (including SCI grouped, by the Responsible Entity, in the Physical Access Control Systems it supports) that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Rationale

Modified to add VCA and SCI as two other forms that a PACS can take. PACS also include the SCI grouped by the Responsible Entity with a virtualized PACS it supports.

Physical Security Perimeter (PSP)

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Rationale

The PSP definition is changing to add SCI as type of device which must be within a PSP.

Protected Cyber Asset (PCA)

One or more Cyber Assets or Virtual Cyber Assets that:

- Is within an Electronic Security Perimeter, but is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter; or
- Share CPU or memory with any part of a BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to the ESP.

Rationale

The PCA definition is being updated to include “share CPU or memory with any part of a BES Cyber System” to mitigate the risks of hardware-based vulnerabilities (Spectre, Meltdown, Rowhammer, etc.) on Shared Cyber Infrastructure for any virtual machines allowed to run on the same hardware as BES Cyber Systems. Since virtualization can allow systems of differing trust levels to simultaneously execute on the same hypervisor servers in the hardware underlay and thus share the same CPU and memory, this addition to the PCA definition requires that those VCAs that do share CPU and memory with a BCS become associated PCA’s of the BCS. This provides the high water marking of VCAs sharing a single hypervisor’s CPU or memory. Affinity rules can be used within the virtualization configuration to prevent this situation and keep other VCAs from becoming associated PCAs. Finally, the definition is being modified to account for “remediation VLAN” automation of security controls where a VCA may instantiate in a logical network reserved for vulnerability assessment and updates (OS patches, AV updates, etc.).

The intent is the VCA does not become a PCA while temporarily in this state as its being updated prior to being connected to its production network.

Removable Media

Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, Shared Cyber Infrastructure, a network within an ESP, or a Protected Cyber Asset.

Rationale

The Removable Media definition is being updated to add SCI as a target of the Removable Media connection.

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:
- A BES Cyber System that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BES Cyber System;
- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or
- Shared Cyber Infrastructure supporting a BES Cyber System.

Rationale

This definition is being modified to add compromised or disrupted SCI supporting a BCS as a target.

Transient Cyber Asset (TCA)

A Cyber Asset or Virtual Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. connected for 30 consecutive calendar days or less:
    - to a network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or
    - directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a:
        - BES Cyber Asset,
        - Shared Cyber Infrastructure, or
        - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Virtual machines hosted on a physical TCA can be treated as software on that physical TCA.
Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Rationale

The TCA definition is being updated to add VCA as a form a TCA can take. The intent is to handle VCAs that are created for typical TCA uses but are normally dormant (e.g. a VCA with Wireshark for troubleshooting network issues within a virtualized infrastructure). Additionally, SCI was added as a target to which TCA's can be directly connected. The statement "Virtual machines hosted on a physical TCA can be treated as software on that physical TCA" is to clarify that on a physical TCA (laptop) with hypervisor software and one or more VCA images, the hypervisor and VCAs are treated as software on the one physical TCA. This is to clarify that the one physical TCA does not have to be tracked simultaneously as multiple distinct virtual TCAs. Corresponding clarifications have been made to the methods in CIP-003 and CIP-010 used to mitigate the risks of TCA software.

Proposed New Terms:

CIP System

A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.

Rationale

This term was created to simplify applicability when referring in the standards or other definitions to objects in scope of the NERC CIP standards in any form they may take (CA, VCA, SCI). It also simplifies applicability when a referral to a "non-CIP System" is needed. If other object types are needed in the future, their addition to this one definition can reduce needed edits throughout the standards.

Cyber System

A group of one or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.

Rationale

This proposed new term is used to simplify applicability when referring in the standards or other definitions to all the forms an object may take (CA, VCA, or SCI). If other forms are needed in the future, their addition to this one definition can reduce needed edits throughout the standards.

Management Interface

A user interface, logical interface, or dedicated physical port that is used to:

- Control the processes of initializing, deploying, and configuring SCI; or
- Provide lights-out management capabilities; or
- Configure an ESP;

excluding physical user interfaces (e.g., power switch, touch panel, etc)..

Rationale

This term is being defined so that requirements can be addressed to SCI and EACMS Management Interfaces to target the unique risks for virtualized environments presented by the management ‘consoles’ for such environments. With ‘infrastructure as a service’ (IaaS) environments, the management consoles can not only be used to create, but also to destroy or reconfigure virtual servers, networks, switches, firewalls, etc. The term also includes interfaces commonly known as ILO (Integrated Lights Out), that can be used to remotely manage hardware (usually including power on/off, access to the physical console, etc.). It also includes interfaces used to configure an ESP (such as on firewalls or a network switch that is enforcing an ESP between different logical networks (e.g., VLANs).

Shared Cyber Infrastructure (SCI)

One or more programmable electronic devices, including the software and Management Interfaces, that share:

- CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, or PACS; or
- storage resources with any part of a BES Cyber System or their associated EACMS or PACS

Each SCI is either:

- included in one or more BES Cyber Systems, EACMS, or PACS; or
- identified independently.

SCI does not include the supported VCA or CA with which it shares its resources. .

Rationale

The SCI definition is being created to separate the underlying hardware from the VCAs that it hosts. This allows security requirements to be targeted to SCI to address the unique risks of virtualization and shared hardware. There are many requirements that now include the newly defined term SCI in the “Applicable Systems” column to maintain security level parity with traditional Cyber Assets.

Beyond security level parity with protecting a typical hardware based Cyber Asset, the SCI can have a more significant impact in a virtualized environment since it can host, and therefore impact, multiple virtualized systems. Because of this capability, some additional controls only apply to SCI, such as the management plane isolation required by the proposed CIP-005. Addressing these unique risks requires separation of the hardware underlay into a separate definition.

The second set of bullets in the definition outlines two options for identifying SCI. Please see the CIP-002-7 Technical Rationale document for a discussion of these options.

The phrase “SCI does not include the supported VCA or CA with which it shares its resources” is included to clarify that, for example, electronic access to a hosted VCA by a user is not electronic access to the SCI on which it executes.

Of note is that shared network devices are not in the scope of this definition. Since network switches and firewalls share their resources by nature, this exclusion avoids pulling all network hardware into scope as SCI. However, network switches and other hardware that does enforce an ESP (such as a network switch configured to logical isolate different VLANs) comes into scope as an EACMS.

Virtual Cyber Asset (VCA)
A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure or a Cyber Asset.

Rationale

The NERC Glossary definition of Cyber Asset has a direct tie to the hardware on which it relied. This affected the definitions of the “Applicable Systems” terms such as BES Cyber Systems (BCS), EACMS, PACS, and Protected Cyber Assets (PCAs). Because the Reliability Standard is applicable to the aforementioned systems, the control for the Cyber Assets also applies to the hardware. This one-to-one relationship between a Cyber Asset and its underlying hardware is what virtualization intentionally breaks to increase reliability and resiliency by allowing Virtual Cyber Assets to be abstracted from the hardware and therefore able move to any available hardware out of a pool of resources.

The proposed NERC Glossary definition of Virtual Cyber Asset (VCA) allows the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined. The definition of VCA is not inclusive of hardware, and other related definitions (EACMS, PACS, PCA, TCA, etc.) have been updated to allow for VCA versions. With the addition of SCI and revisions to the “Applicable Systems”, there can be one or more virtualized instances (each a VCA) of a BCA, EACMS, PACS or PCA that reside on SCI.
Examples of Virtual Cyber Assets may include, but are not limited to, logical instances of the following:

- Operating Systems (Virtual Machines (VM));
- Networking devices such as switches, routers, and load balancers;
- Security appliances such as firewalls and VPN concentrators; and
- Helper appliances with logical connectivity (such as malware detection, plugins, etc.).

Proposed Retired Terms:

None

Technical Rationale for Exemptions Section:

Rationale for Exemption 4.2.3.1

The term ‘Cyber Assets’ was changed to ‘Cyber systems’. Rather than changing this language to a list of all possible forms (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure) as the object of the exemption, the SDT chose to instead use the existing language in the 4.2.3.4 and 4.2.3.5 exemptions such that all five exemptions use ‘systems’ as their object.

Rationale for Exemption 4.2.3.2 and 4.2.3.3

In 4.2.3.2, the term ‘Cyber Assets’ was changed to ‘Cyber Systems’ which is a new proposed glossary addition. Rather than changing these two exemptions to list all possible forms (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure), the SDT chose to define a new term that incorporates all forms and use it within the multiple exemptions and at other points within the standards.

For 4.2.3.3, the ability to move workloads or VM's seamlessly across different sites for increased resiliency can require different sites to be connected as a flat network without layer 3 ESP's at each discrete site (e.g., a layer 2 adjacency across the sites). A "Super ESP" as its been historically known is created across the sites and thus an exemption based on having a discrete layer 3 ESP at each site no longer works to exclude, for example, the network transport equipment belonging to carriers.   The SDT is including the 4.2.3.3 exemption to further clarify this scenario. Responsible Entities should notice the exemption uses the word "between" – when extending an ESP between geographic locations, CIP-005 requires the confidentiality and integrity protection of the data (typically through encryption) between the relevant PSPs. This exemption then covers the related Cyber Systems "between" those encryption points but does not exclude the endpoints performing the encryption.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — BES Cyber System Categorization

Technical Rationale and Justification for Reliability Standard CIP-002-7

June 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-002-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-002-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-002-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a SDT. The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 Part 1.1-1.3

Change Rationale:

The SDT has modified these requirement parts such that identification of Shared Cyber Infrastructure (SCI) that hosts high impact BES Cyber Systems (BCS) (Part 1.1) and medium impact BCS (Part 1.2) is included in the existing Requirement Parts. SCI can host not just a single but multiple BCS, Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), Protected Cyber Assets (PCA), etc. of varying impact levels or association to a BCS. As such, they may present a higher level of risk than a single BCS and are to be identified for the application of requirements in the remainder of the CIP standards.

The SDT modified the requirement parts to allow Responsible Entities options in how they identify and group virtualized systems. The two bullet points (this example will use Requirement R1 Part 1.1 for high impact) are designed to allow:

- A high impact BCS including any supporting SCI identified as part of the BCS; or
    - This option is known as the "All-in Option". In this option, if any part of the BCS is virtualized the underlying SCI is identified and included in the composition of the entity's BCS.

- A high impact BES Cyber System and independent SCI supporting any part of the high impact BES Cyber System or its associated EACMS, PACS, or PCAs.
    - This option is known as the "Identified SCI option". In this option, if any part of the BCS is virtualized it allows the entity to identify its high impact BCS (including any Cyber Assets and Virtual Cyber Assets (VCA)), however the underlying SCI is identified separately as a distinct object that is not a part of a hosted BCS.

See discussion below for the rationale behind the two options for identifying virtualized system's SCI and considerations for choosing one over the other.

Options For Identifying Virtualized System's SCI

The SDT has modified CIP-002 to allow Responsible Entities a choice between two options for identifying the SCI supporting virtualized systems. These two options represent two different ways entities may treat SCI within their programs. One allows for a simpler identification exercise but then limits the flexibility of the impact classification of the VCAs hosted on the SCI, while the other allows for more flexibility in the impact classification of the VCA's hosted on the SCI, but requires a slightly more complex identification process. These two options have come to be known as the "All-in" or the "Identified SCI" options. In either option, the security requirements within the standards are equivalent for the SCI itself; the difference in the options is the level of flexibility in categorizing VCAs hosted on the SCI.

All-in Option

This option would typically be chosen by entities that have SCI dedicated to a BCS environment of a single impact category. The entity identifies their BCS and its Cyber Assets, VCA, and any associated SCI all as part of one or more BCS of the same impact category. However, since the SCI is part of the BCS, every VCA hosted on the SCI is either a BCA of the same impact as the BCS or an associated PCA of the highest impact BCS hosted on the SCI. Thus the name "All-in"; the SCI and all VCAs hosted on it are all high watermarked as the SCI is identified as a component of the BCS.

Identified SCI Option

This option would typically be chosen by entities that use their SCI to support a broader range of VCAs than just BCS of a single impact category. They may desire to use the tools and security controls available within their SCI to logically segment/isolate these varying systems of differing impact levels without having to consider everything hosted on an SCI as an associated PCA and thus high watermarking the SCI and everything it hosts. In this option, the entity would identify their SCI independently and **not** as a a part of any BCS. The SCI in this option is a separate object that may host high, medium, low, or no impact cyber systems with the proper security controls and logical isolation in place between these impact categories to meet the CIP requirements.

Requirement R1 Part 1.3

Change Rationale:

The SDT modified Requirement R1 Part 1.3 to include the identification of "asset that contains" to include low impact BCS as well as SCI that supports any portion of a low impact BCS. This modification was made because SCI, which can host multiple BCS, may pose a greater risk to the BES than a single BCS. Additionally, the term Cyber Asset was modified to exclude SCI so that SCI could could be addressed separately from any hosted VCAs. Responsible Entities should note that the definition of SCI contains its associated Management Interface, thus an "asset that contains" could be a location of the Management Interface used to manage a distributed SCI.

For example, hypervisors within one SCI may be distributed across numerous assets such as substations, generating sites, or control centers and the Management Interface for the SCI could be located at yet another location. With this change, the rationale is the "asset" containing the Management Interface becomes important as it relates to potential impact to the low impact BCS and would be another identified entry on the Responsible Entity's evidence for

Requirement R1 Part1.3 that is later subject to controls in CIP-003 Requirement R2 that parallell those for the asset containing the low impact BCS.

Attachment 1 – Impact Rating Criteria

Change Rationale:

In the medium impact rating criterion 2.1 referencing shared BCS for commissioned generation, the SDT has proposed a change to incorporate an earlier approved Request For Interpretation (RFI). The RFI was submitted seeking clarification of Criterion 2.1 of Attachment 1 regarding the use of the phrase “shared BES Cyber Systems.” The resulting approved interpretation was introduced as Appendix 1 in CIP-002-5.1a.

The SDT incorporated the interpretation into CIP-002-7 Attachement 1 criterion 2.1 by modifying it to reference “each discrete shared BCS” and removed the RFI appendix from the standard.

Former Background Section from Reliability Standard CIP-002-5.1a

The **Background** section has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

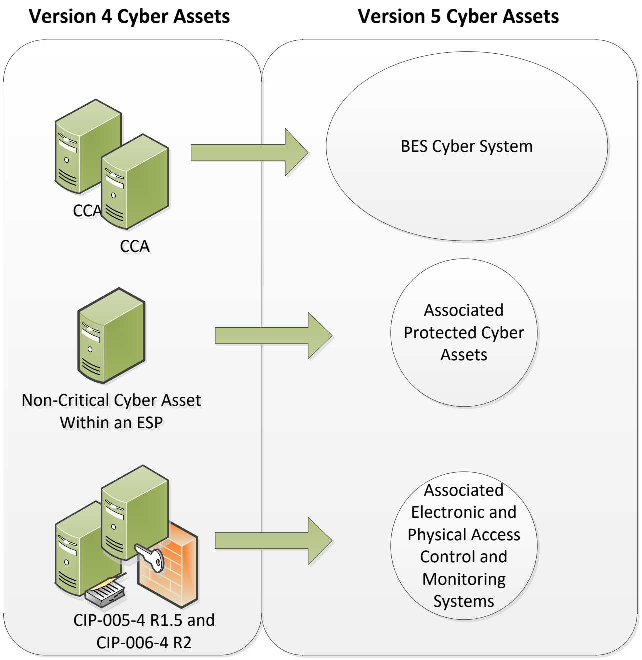
This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an “or,” and numbered items are items that are linked with an “and.”

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team’s review of the NIST Risk Management Framework and the use of an analogous term “information system” as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the “BES Cyber System” term primarily

to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term “BES Cyber System” is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity’s responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than “Real-time,” BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS")

Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")

Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA")

Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

Technical Rationale for Reliability Standard CIP-002-5.1a

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from the CIP-002-5.1a standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1a

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints

- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
    - Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)

        - Special Protection Systems or Remedial Action Schemes
    - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
        - Under and Over Frequency relay protection (includes automatic load shedding)
    - Sensors, relays & breakers (DP)
        - Under and Over Voltage relay protection (includes automatic load shedding)
    - Sensors, relays & breakers (DP)
        - Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
    - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
    - Software used to perform calculation (BA)
- Demand Response
    - Ability to identify load change need (BA)
    - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
    - Ability to identify load change need (BA)
    - Ability to implement load changes (TOP, DP)
- Non-spinning reserve (contingency reserve)
    - Know generation status, capability, ramp rate, start time (GO, BA)
    - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
    - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
    - Software to calculate unit adjustments (BA)
    - Transmit adjustments to individual units (GOP)
    - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
    - Frequency source, schedule (BA)
    - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term “Facilities”, there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports

the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.

- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.

In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.
- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.
- Criterion 2.13 categorizes as medium impact those BA Control Centers that “control” 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.
- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the “Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface.” This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.
- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:
  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

- 230 kV –> 700 MVA
- 345 kV –> 1,300 MVA
- 500 kV –> 2,000 MVA
- 765 kV –> 3,000 MVA

In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

- For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.
- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.
- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.
- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.
- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.
- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

  In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.
- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that “control” 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC’s Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

  Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

  BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator’s restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator’s restoration plan. The glossary term Blackstart Capability Plan has been retired.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to “provide the entities identified in

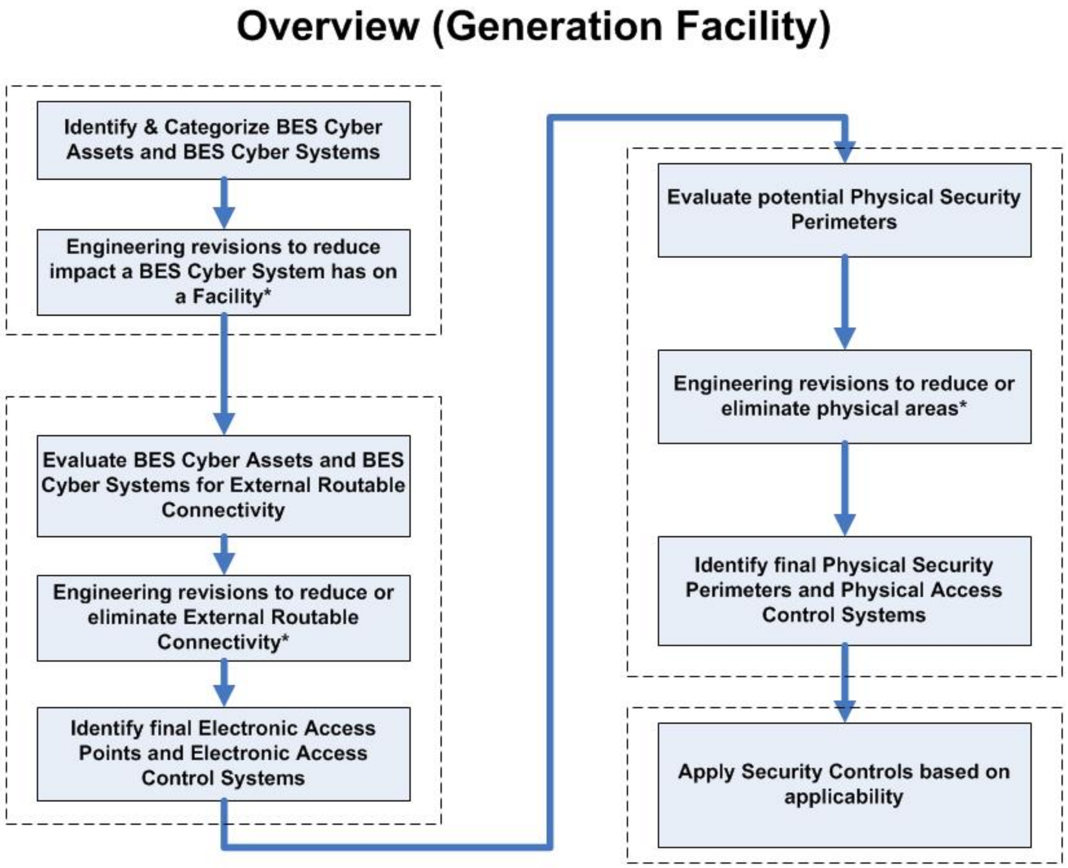
its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Appendix 1

Requirement Number and Text of Requirement

CIP-002-5.1, Requirement R1

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

- i. Control Centers and backup Control Centers;
- ii. Transmission stations and substations;
- iii. Generation resources;
- iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

Attachment 1, Criterion 2.1

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions

Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."

The Interpretation Drafting Team identified the following questions in the RFI:

1. Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?
2. Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?
3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

Responses

Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)

Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:

> The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term “shared” is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.” For criterion 2.2: “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-Y

June 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-003-Y

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-9. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-Y is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document stated, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to shorten applicability statements within the body of CIP standards with “BCS” as the defined acronym for “BES Cyber System”. The SDT added the option (known as the “all-in” scenario) for entities to group SCI within a BCS it supports; Therefore, no other changes were necessary in Requirement R1 (See the CIP-002 Technical Rationale document for a description of the options for identifying SCI and reasons an entity may choose between the options).

Requirement R2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to align security management control requirements with the virtualization changes.

To ensure SCI supporting low impact BCS is afforded equal physical security controls as the BCS, the SDT changed “their associated SCI” to “SCI that supports any part of a low impact BCS”, and included the same exclusions regarding discrete lists for low impact BCS as well as the supporting SCI as identified in CIP-002.

Attachment 1 Section 2

Rationale

To ensure SCI that supports any part of a low impact BCS is afforded equal physical security controls as the BCS, the SDT added “the asset or the locations of the SCI hosting low impact BES Cyber Assets within the asset.”

Additionally, to ensure virtual infrastructure providing electronic access controls for the low impact BCS is afforded equal physical security controls as the physical Cyber Assets that provide electronic access controls for the low impact BCS, the SDT modified this section to include the Virtual Cyber Asset (VCA) where only Cyber Assets had previously been listed.

Attachment 1 Section 3

Rationale

To ensure an asset containing a low impact BCS or an SCI supporting a low impact BCS is afforded equal electronic access controls as the low impact BCS, the SDT added “SCI that supports any part of a low impact BCS” as identified in CIP-002.

Attachment 1 Section 3 Part 3.1

Rationale

Part 3.1(i) To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a system(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term system(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Part 3.1(ii) To ensure only necessary inbound and outbound electronic access is permitted for SCI hosting a low impact BCS just as is required for access control to the low impact BCS, the SDT adjusted the language to include communications that are between SCI that supports any part of a low impact BCS and a system(s) outside the asset(s) containing the SCI that supports any part of a low impact BCS.

Part 3.1 (iii) To ensure SCI supporting low impact BCS is afforded equal electronic access controls for routable communications entering or leaving the asset containing the low impact BCS, the SDT added “the asset containing the SCI that supports any part of a low impact BCS" to the low impact BCS. Also, in the interest of brevity and consistency, examples were removed from the requirement language in favor of deference to Implementation Guidance where such examples exist.

Attachment 1 Section 3 Part 3.2

Rationale

To ensure SCI supporting low impact BCS are afforded equal electronic access controls for Dial-up Connectivity, the SDT added "the asset containing the SCI that supports any part of a low impact BCS" to the low impact BCS. Per VCA capability was included in addition to per Cyber Asset capability to accommodate for incapability of both physical and virtual aspects of the low impact BCS or its associated SCI.

Attachment 1 Section 5

Rationale

To ensure SCI supporting a low impact BCS are afforded equal mitigations from the introduction of malicious code as the low impact BCS, the SDT added "SCI that supports any part of a low impact BCS" to the low impact BCS.

Attachment 1 Section 5 Part 5.1

Rationale

To enable for virtualization technologies and capabilities the SDT added, "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code" as an option in Attachment 1 Section 5 Part 5.1.

Attachment 1 Section 5 Part 5.2

Rationale

To ensure SCI supporting a low impact BCS are afforded equal protections when a TCA managed by a party other than the Responsible Entity is used, the SDT added "SCI that supports any part of a low impact BCS" to the low impact BCS in Attachment 1 Section 5 Part 5.2.1.

To enable for virtualization technologies and capabilities the SDT added, "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code" as an option in Attachment 1 Section 5 Part 5.2.1.

The final bullet of Attachment 1 Section 5 Part 5.2.1 was preceded with the language "Review of" to make the requirement for other methods parallel to the five options listed above it.

Attachment 1 Section 5 Part 5.3

Rationale

To ensure SCI supporting a low impact BCS are afforded equal protections from malicious code when using Removable Media, the SDT added "SCI that supports any part of a low impact BCS" to the low impact BCS in Attachment 1 Section 5 Parts 5.3.1 & 5.3.2.

Former Background Section from Reliability Standard CIP-003-8

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Technical Rational for Reliability Standard CIP-003-8

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-003-8 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC’s cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization’s internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access

For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity’s security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only “necessary” inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

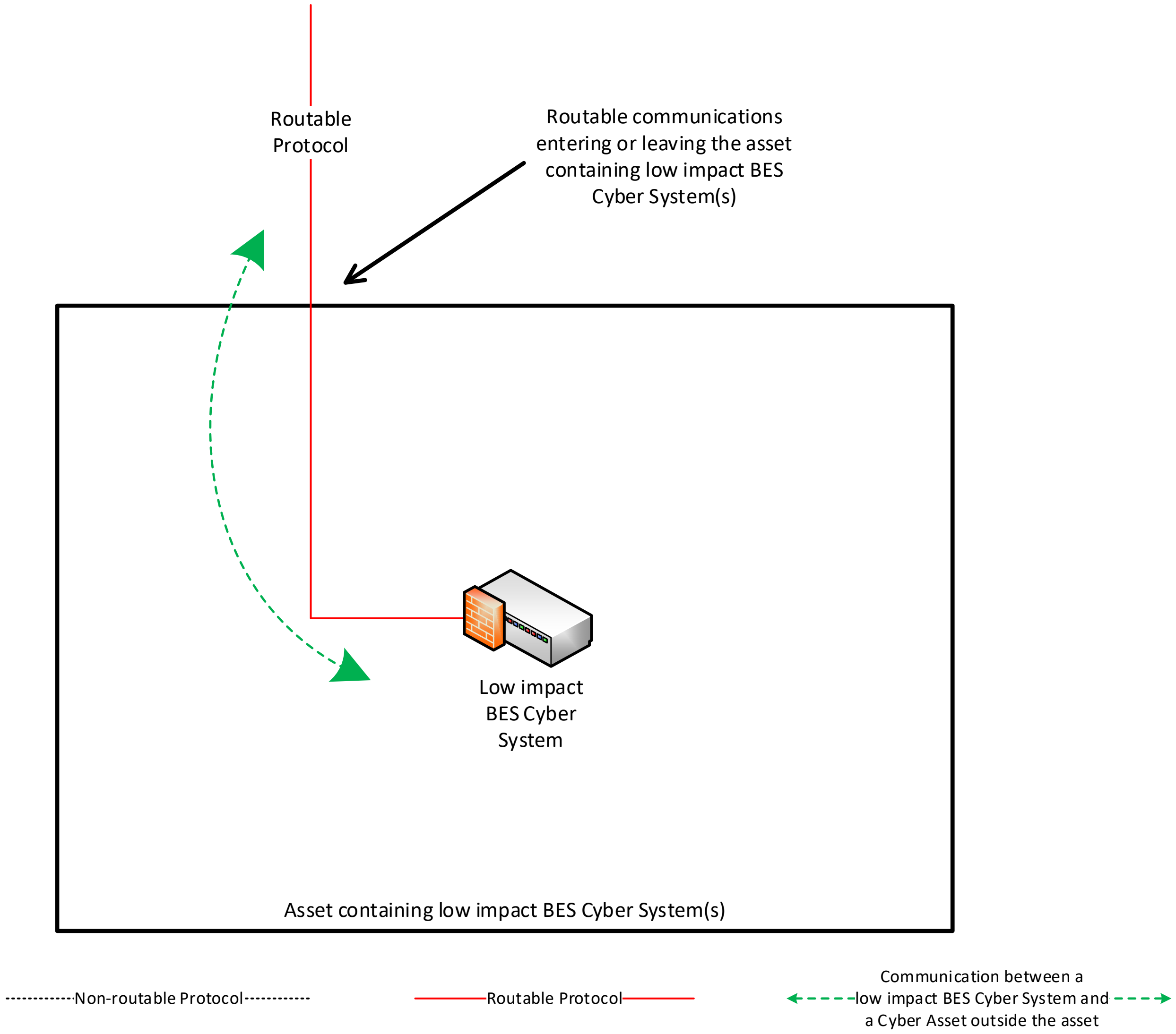
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

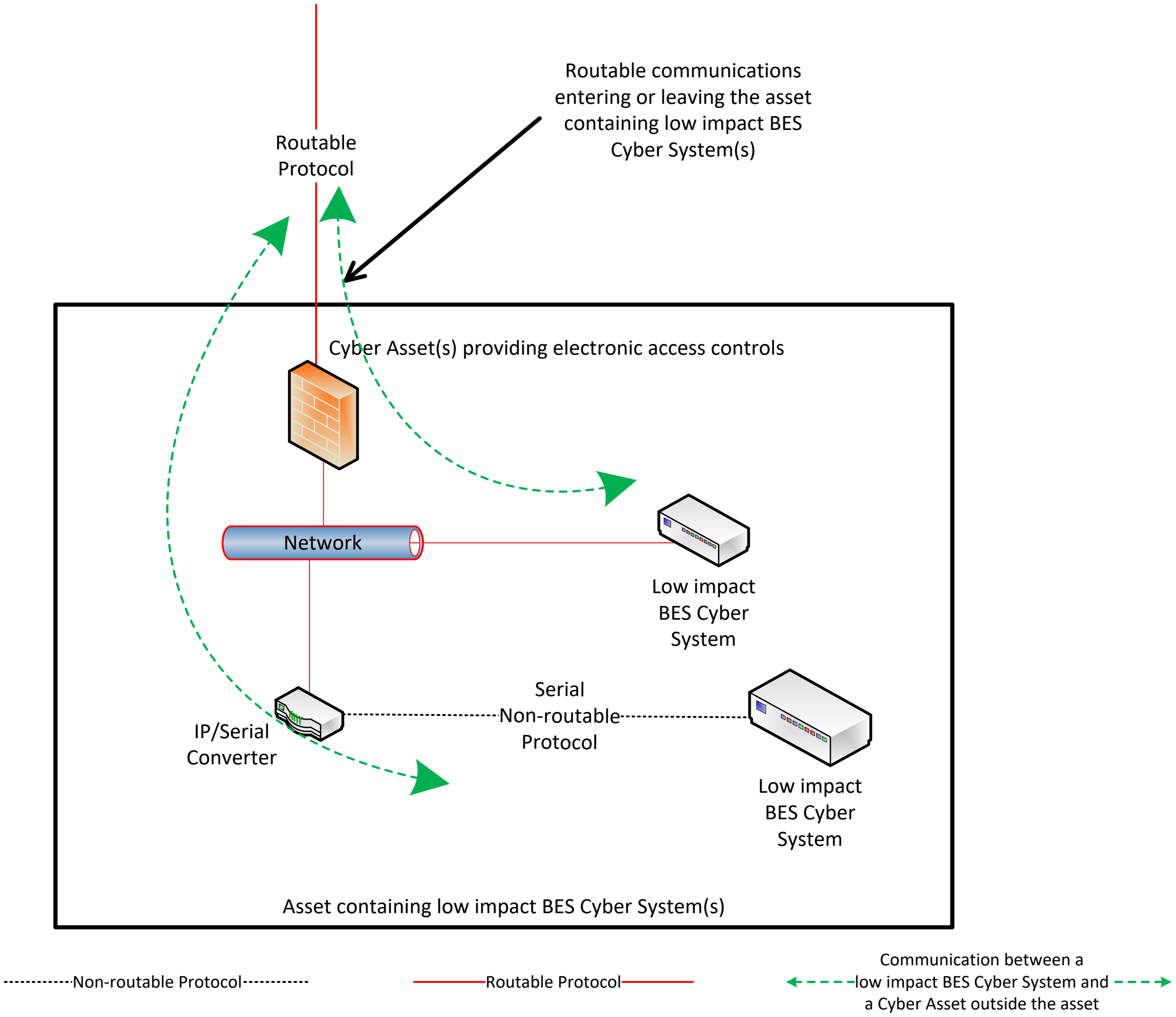
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

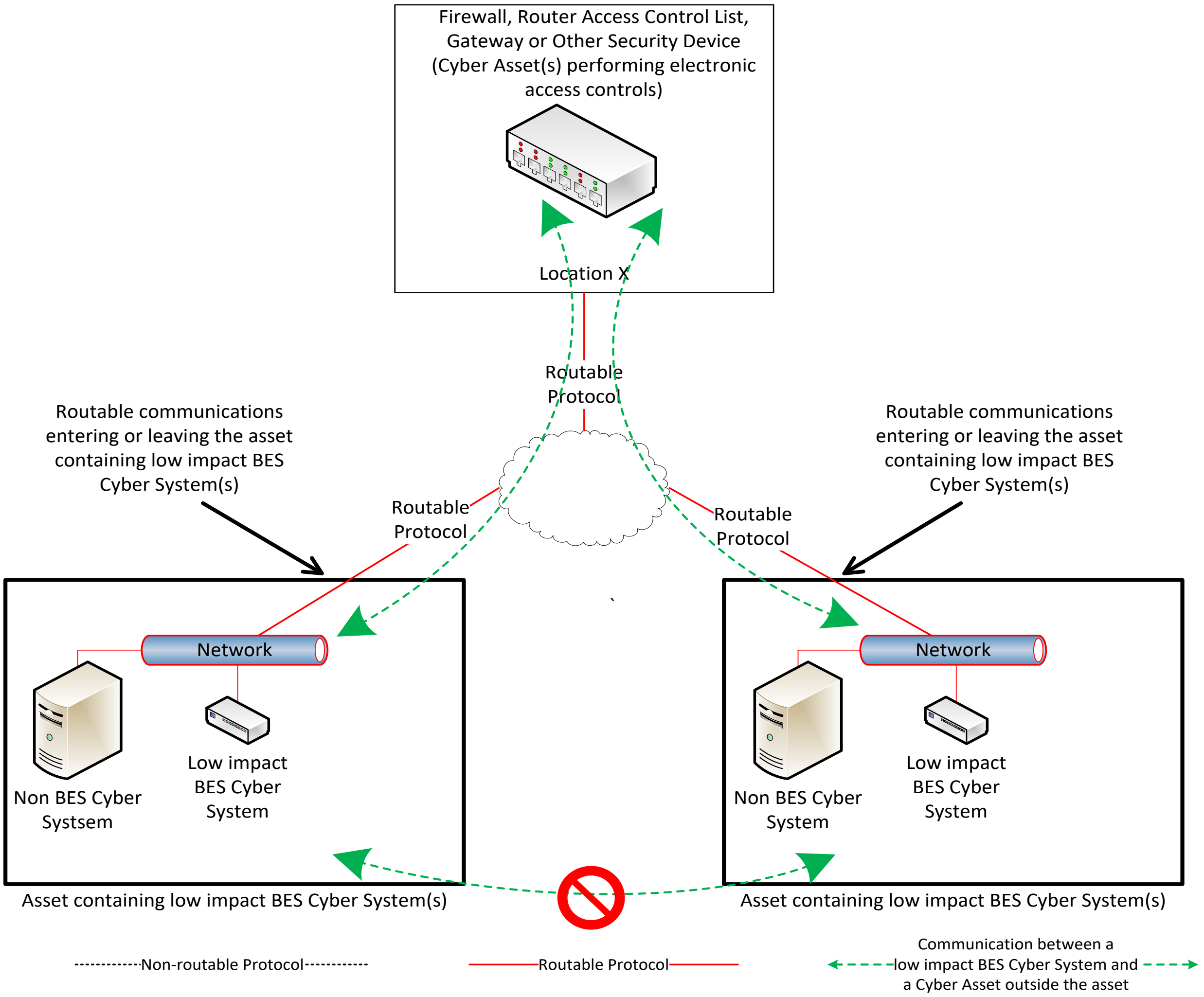
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

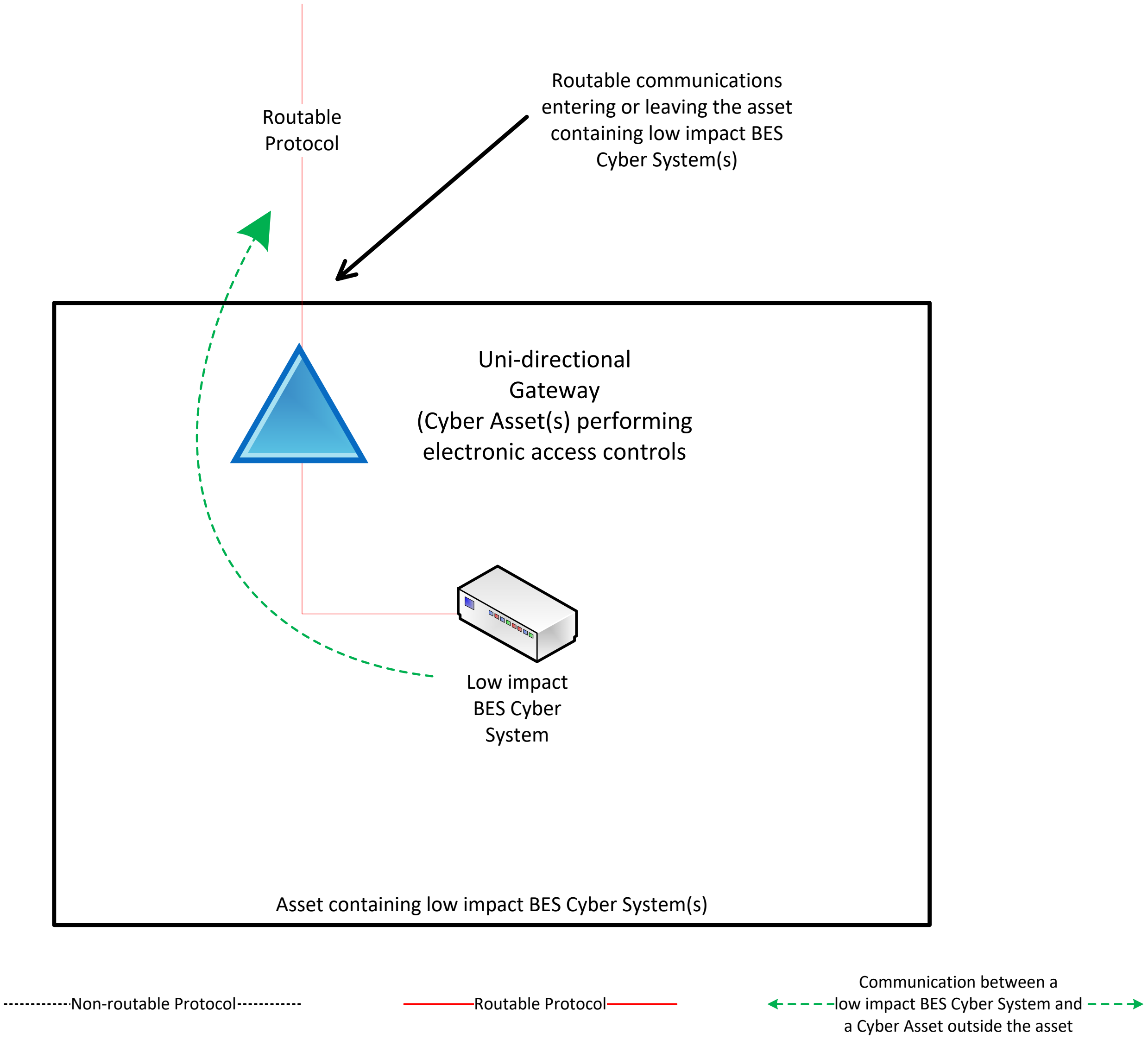
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

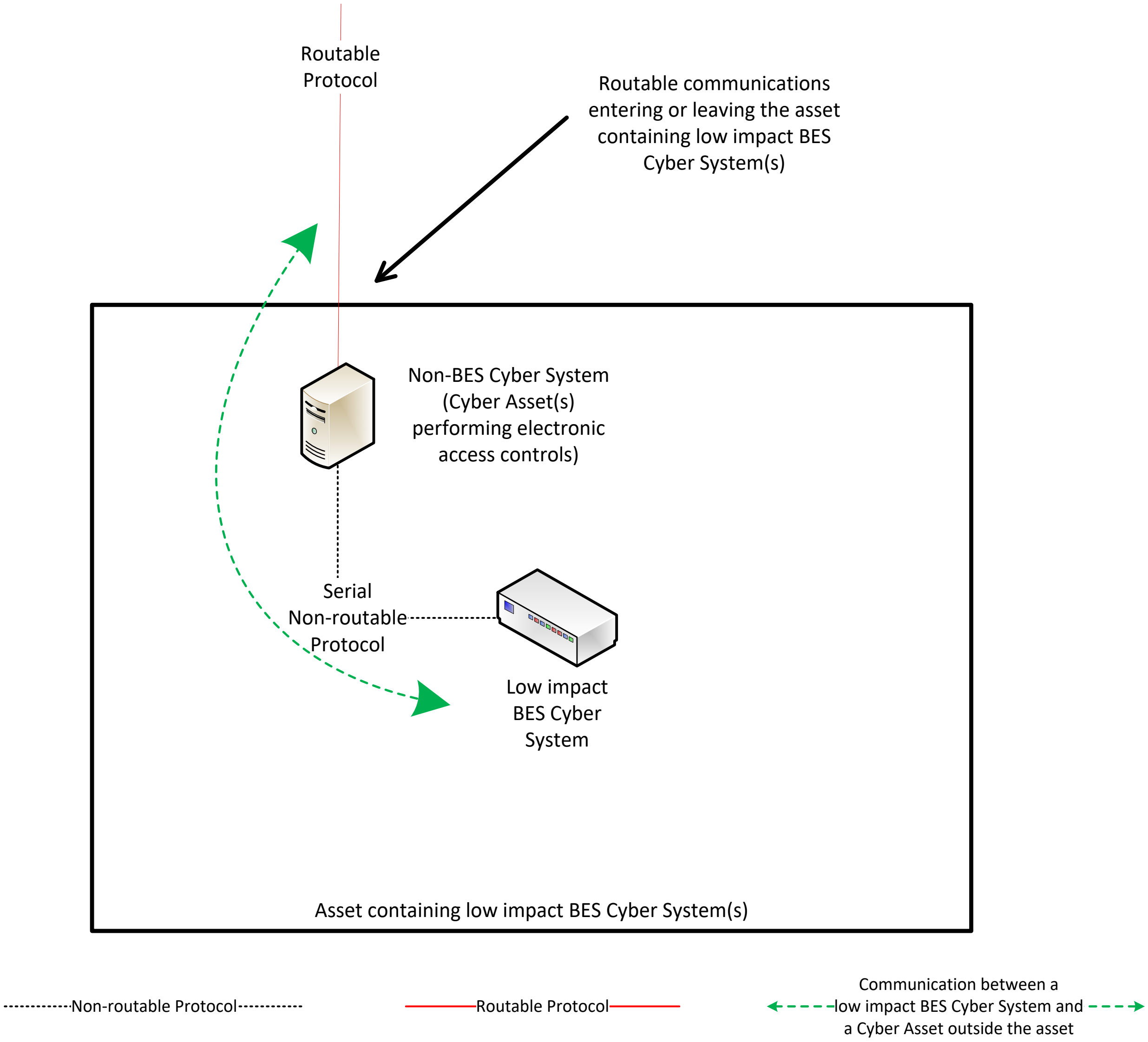
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a “one-way” (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

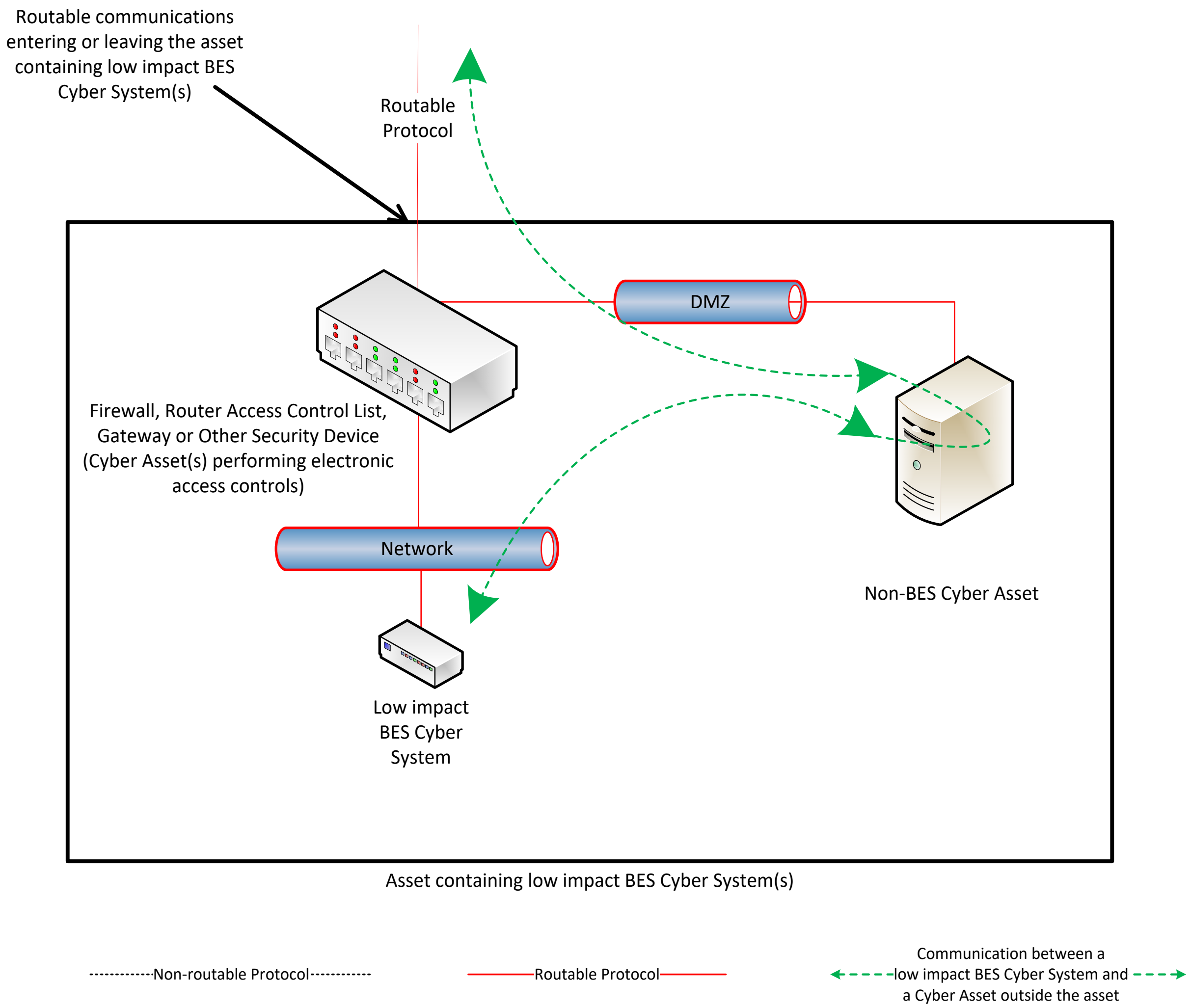
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

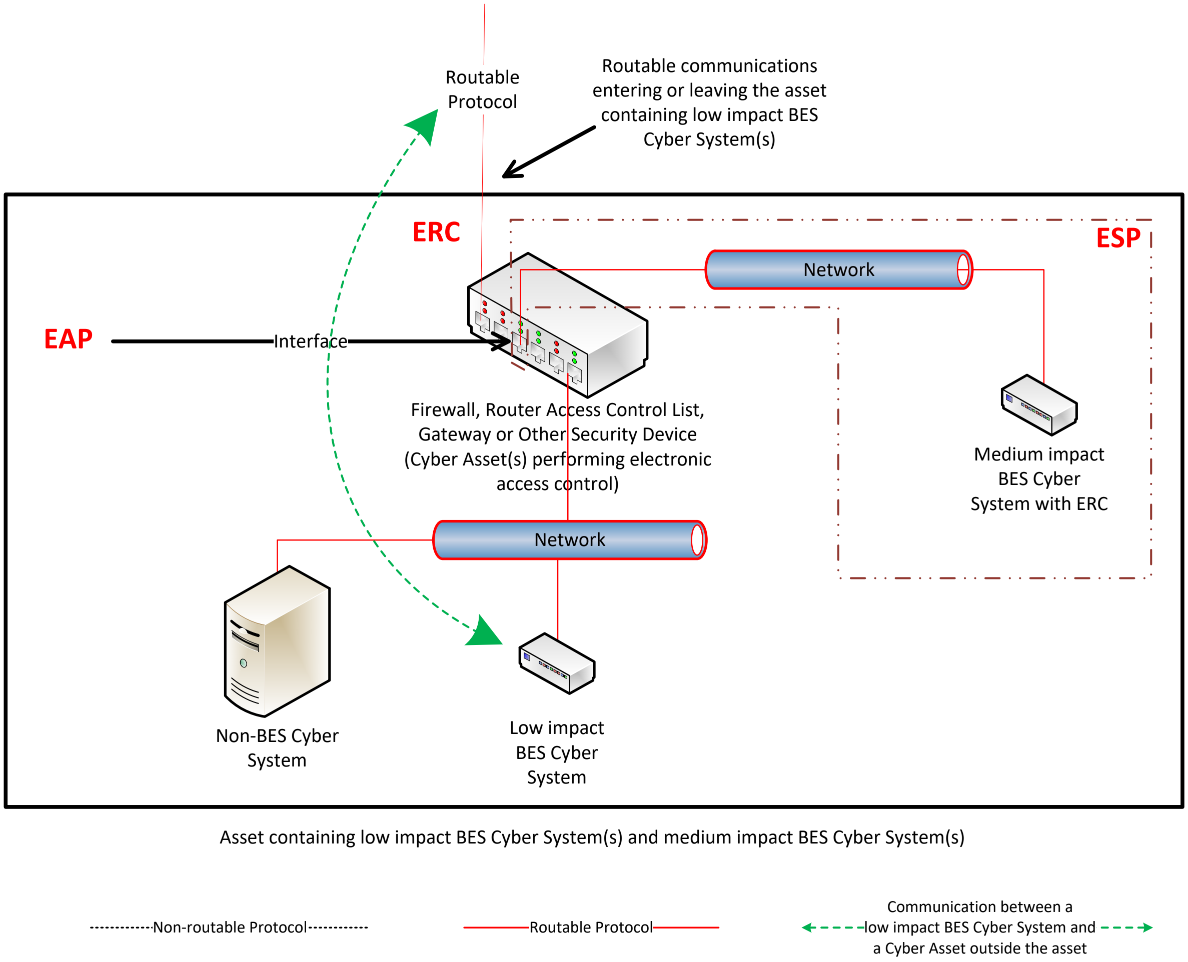
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.



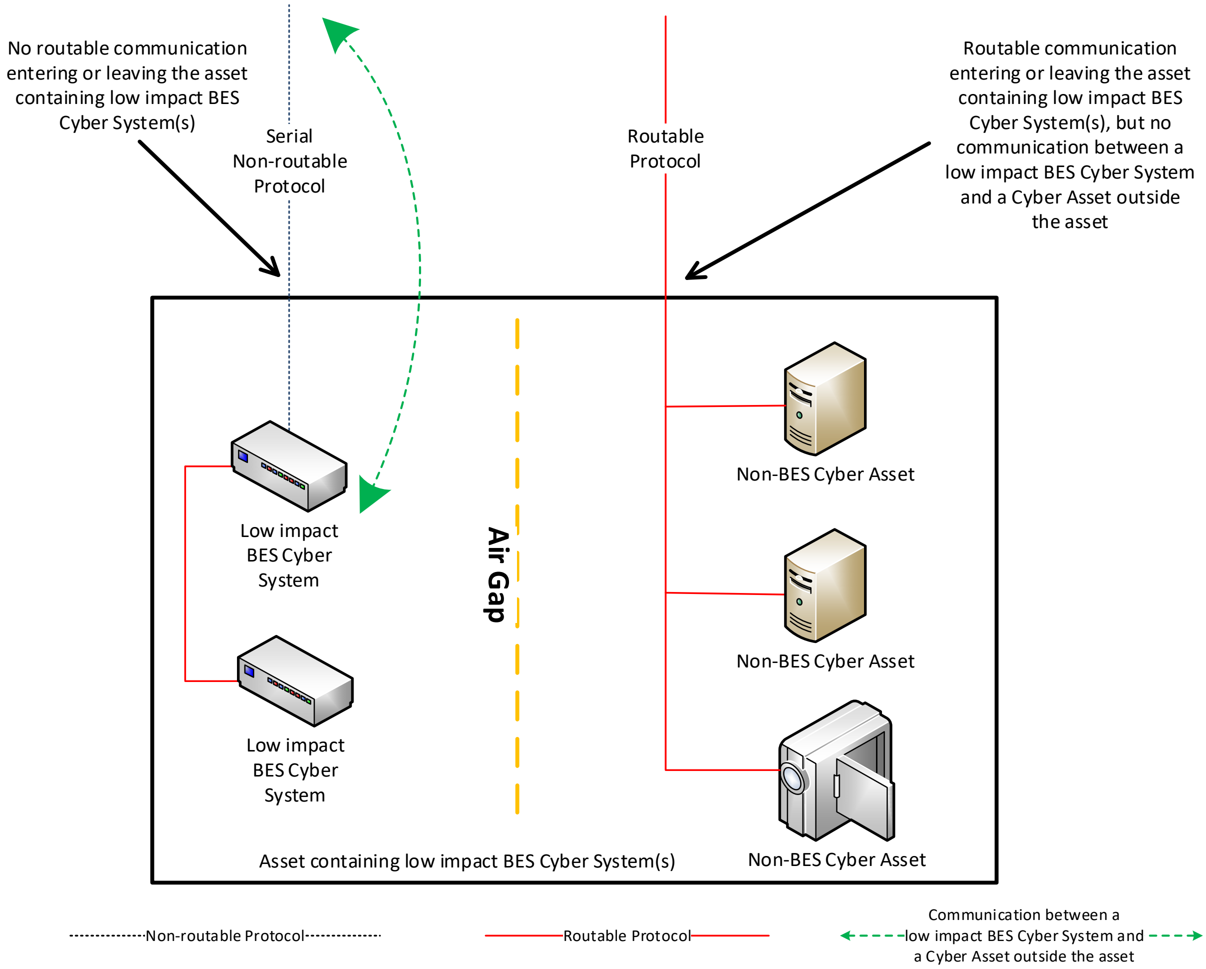
Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1. The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2. The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3. The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).

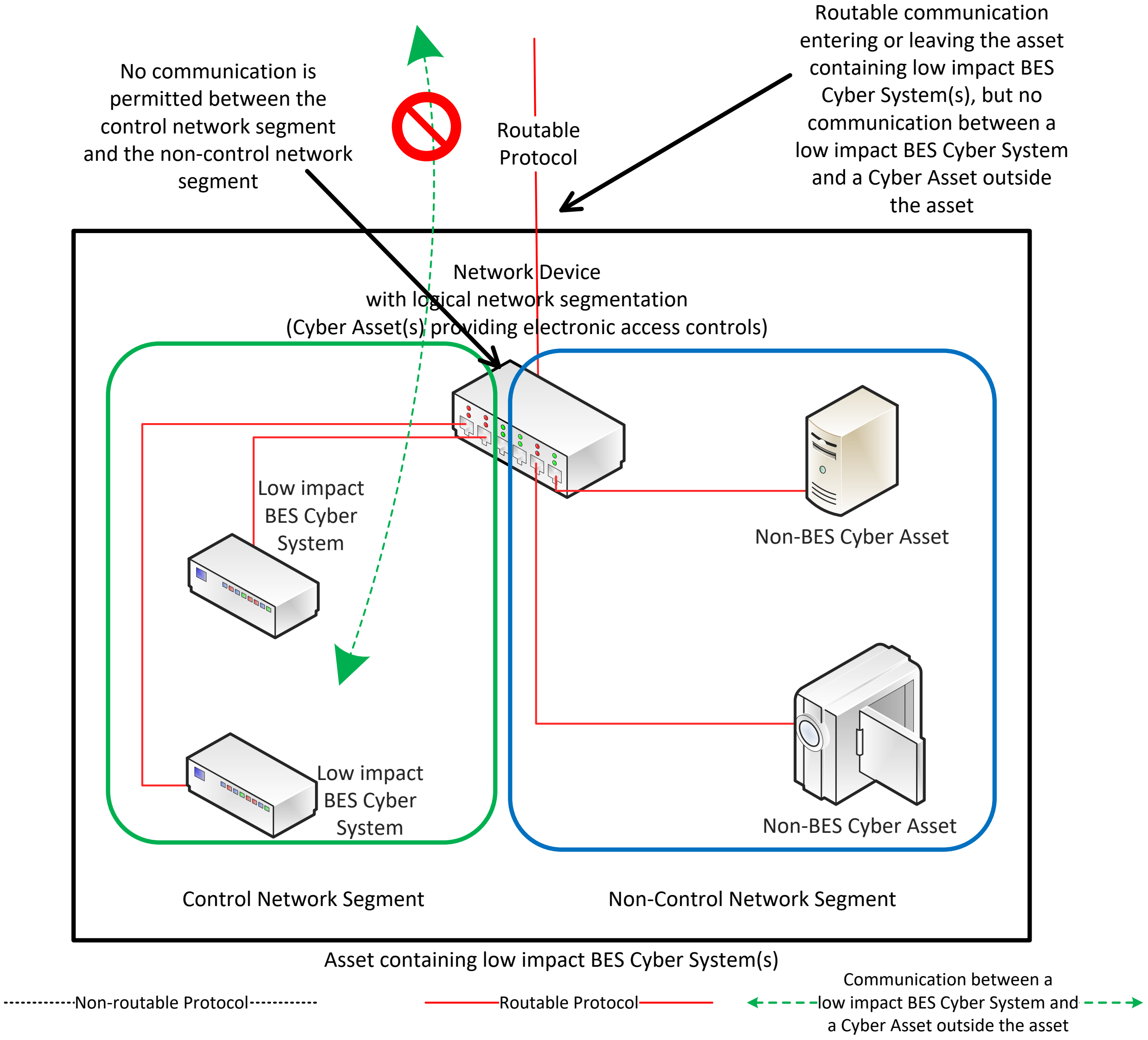
Section 1.



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

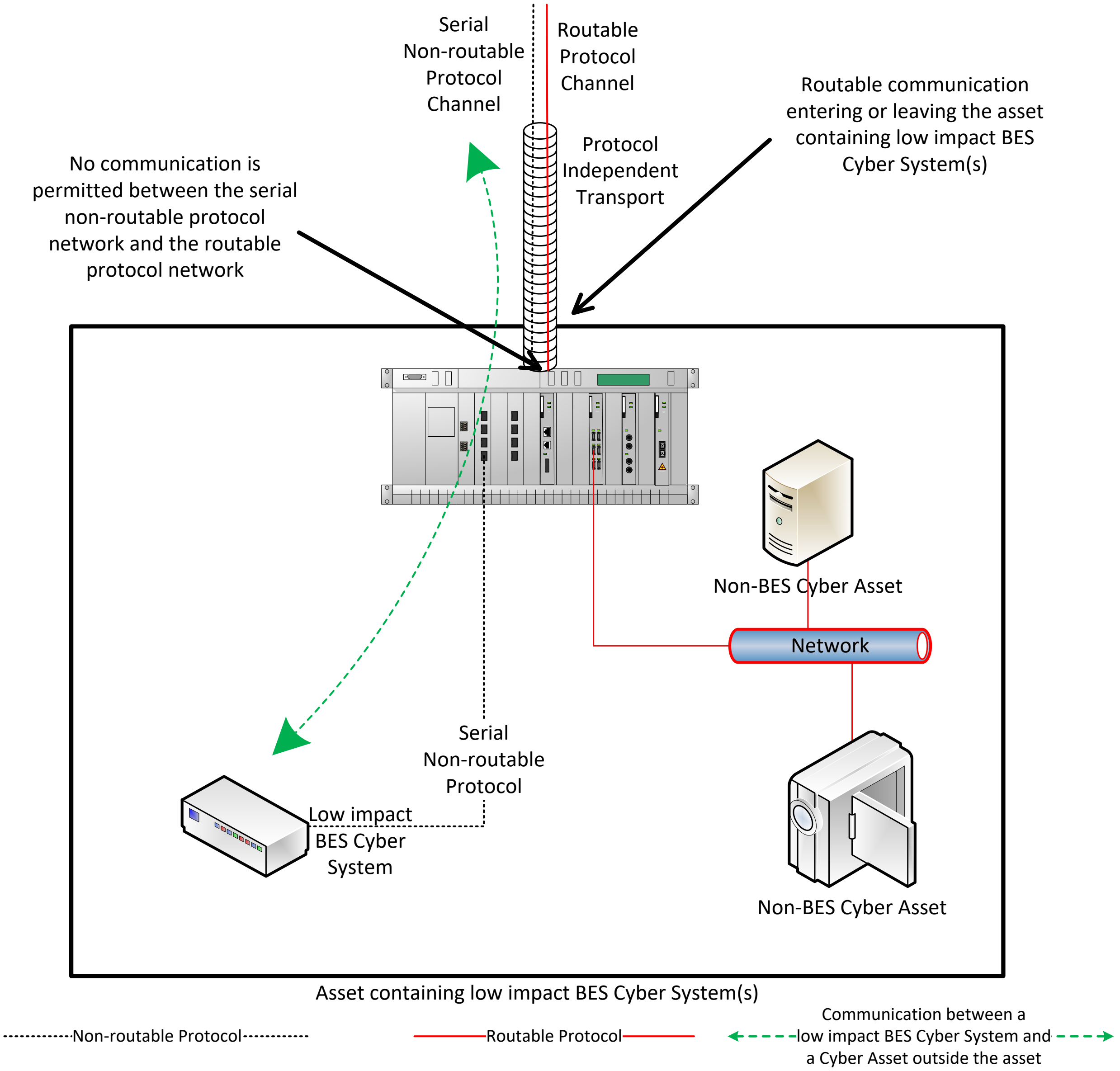
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity’s response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, “A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.” The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity’s responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party’s security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of “prior to connecting the Transient Cyber Assets” is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2.1: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Section 5.2.2: The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

---

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious

Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):
Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):
Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies

required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for “clear lines of authority and ownership for security matters.” With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-Y

June 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-004-Y

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-Y. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-004-Y is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the issues identified by the V5TAG was virtualization. The V5TAG Transfer document states, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." Document for reference when reading the technical rationale that follows.

Requirement R1-R6

General Considerations

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-004-Y to align personnel and training requirements with the virtualization changes.

The SDT added the option (known as the "all-in" scenario) for entities to group SCI within a BCS it supports; Therefore, to enable CIP-004-Y for virtualization, the SDT added "SCI identified independently supporting an Applicable System above" each of the Parts in Applicable Systems for Requirement R1 – Requirement R6 to account for the alternative option (See the CIP-002 Technical Rationale document for a description of the options for identifying SCI and reasons an entity may choose between the options.)

Additionally, where the term BES Cyber System (BCS) was used in the requirement language, it is replaced with "Applicable Systems" to align the requirement language of each Requirement Part with the updated applicability for each Requirement Part.

Requirement R3 Part 3.5

Summary of Changes:

A CIP Exceptional Circumstance was added as an exception to processes to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed prior to granting authorized electronic access and authorized unescorted physical access.

Change Rationale:

The SDT determined Responsible Entities cannot require personnel risk assessments for first responders prior to granting them authorized unescorted physical access during certain conditions that qualify as CIP Exceptional Circumstances.

Former Background Section from Reliability Standard CIP-004-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]." The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program.

However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

The following conventions are used in the “Applicable Systems” column as described. High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-004-6

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity’s process during the tenure of employment, which may or may not be the same as the initial verification action.

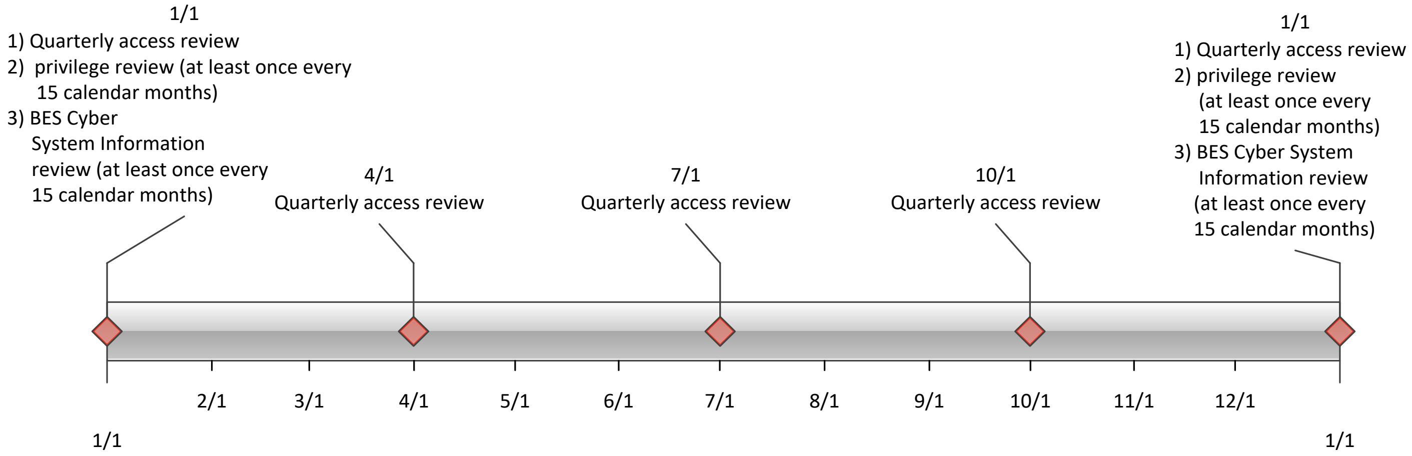
A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.



Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. “Authorization” should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. “Provisioning” should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity’s policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing “immediate” revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the

Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security – BES Cyber System Logical Isolation

Technical Rationale and Justification for Reliability Standard CIP-005-8

June 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-005-8

Introduction

This document is the technical rationale and justification for Reliability Standard CIP-005. It includes the rationale for changes in the current proposed version (CIP-005-8) as well as previous versions of the standard. The intent of this document is to provide stakeholders and the ERO Enterprise with an understanding of the revisions and the technical concepts of the Reliability Standard as well as the rationale for such revisions, both the currently proposed and historical revisions from previous versions and SDTs.

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team’s (SDT’s) intent in drafting changes to the requirements.

Background

The Version 5 Transition Advisory Group (V5TAG), which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry’s implementation activities. During the course of the V5TAG’s activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, “The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005-8 and the definitions of Cyber Asset and Electronic Access Point (EAP) that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies.”

Summary

The Project 2016-02 Standard Drafting Team (SDT) proposal accommodates for increasing use of virtualization and other technology innovation. The SDT’s purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards, but also to better position the CIP standards to be applicable to additional future technological innovation while, to the extent possible, maintaining backwards compatibility.

CIP-005-8 remains a standard concerned with controlling communications to and from BES Cyber Systems by establishing an Electronic Security Perimeter (ESP) with increased security controls for Interactive Remote Access and vendor remote access. However, virtualization is enabling models for network security, such as “Zero Trust”, that are not network perimeter based. Therefore, in CIP-005-8 the ESP is focusing on being a security perimeter rather than a network perimeter. Securing the communications to and from BES Cyber Systems is the security objective, but the standard no longer prescribes “where”, as in where on a network, the controls must be implemented. Innovations such as Zero Trust models are moving access control from network borders to a session level orientation and eliminating the implicit trust within a local network. Network perimeter-based ESP and EAP implementations remain a valid option and are one method for allowing only necessary and controlled communications to the Cyber Systems within the ESP but are no longer the only prescribed option. In combination with an updated, broader ESP definition, CIP-005-8 now focuses on the objective of having policies or configuration in an EACMS that permits only needed communications and denies all other communications.

Another concept introduced within CIP-005-8 is shared infrastructure (defined as Shared Cyber Infrastructure (SCI)). With the introduction of hardware (servers, storage, networks) as a generic infrastructure fabric on top of which virtual cyber systems, networks, and storage locations are built, the need to isolate Cyber Systems from others of different trust levels must move beyond a network only separation. In these virtualized environments where SCI is used, a risk of side channel attacks exists where, for example, a low impact BCS that is isolated from a high impact BCS from a network communication perspective but still shares CPU or memory with the high impact BCS, could be used to attack the high impact BCS through hardware-level vulnerabilities (e.g., Spectre, Meltdown, Rowhammer). CIP-005-8 mitigates this risk by either:

- Using affinity controls within the virtualization environment to configure the hypervisor(s) to disallow Virtual Cyber Assets (VCA) in these differing trust levels from simultaneously executing on the same CPU and memory in the hardware underlay (SCI), or
- Treating all VCA that can simultaneously share the same CPU or memory as associated Protected Cyber Assets (PCA) of the highest impact system (high watermarking) to raise them to the same trust level.

Additionally, the SDT is proposing a new requirement (CIP-005-8 Requirement R1 Part 1.3) to separate the management plane of the Shared Cyber Infrastructure (SCI) from the data plane. This is needed to ensure the reliability and security of the SCI and the VCA's it hosts as the management plane is where network and hardware isolation is configured as well as where the VCAs themselves are created, managed, or deleted.

CIP-005-8 also introduces exemptions and requirements for extending ESPs across different Physical Security Perimeters (PSP) (often known as "Super ESPs"). This is often used to extend a flat network between two virtualization infrastructures (SCI) in two different locations to allow VCAs to seamlessly transfer between SCI at the locations to improve resilience and reliability.

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 General Considerations

ESP Redefinition

Network border-based ESPs and EAPs remain a valid option for controlling the communications to and from BES Cyber Systems. However, virtualization technologies and models such as Zero Trust present equally effective methods that are not based on network border-based solutions dealing only with layer 3 routable protocols. Virtualization and its accompanying SCI have other characteristics such as shared hypervisors, shared storage, shared virtual networks and switches, all of which pose different security concerns but also have their own security controls. To adapt to these changes, CIP-005-8 focuses on an objective-based requirement (in Requirement R1 Part 1.1) for controlling communications. Required ESPs are now more truly security perimeters rather than purely network perimeters and the standard doesn't prescribe a single place the necessary controls must be implemented (a Cyber Asset interface on an EAP on a network border). Models such as Zero Trust can implement more granular controls throughout a network and without regard to network location on a per-access or per-session level.

Shared infrastructure and "Mixed Trust" Risks

For virtualized environments where SCI is used, a risk of side channel attacks exists. Virtualization allows disparate workloads of what could be differing impact or trust levels to execute on the same CPUs and share the same memory (i.e. RAM) within the infrastructure. There are vulnerabilities that are directly related to sharing hardware such as Spectre, Meltdown, and Rowhammer. Rowhammer, for example concerns processes sharing certain forms of hardware memory. Repeated writing of bits in one process could flip bits in a process in adjacent physical memory. This type of vulnerability is one of the unique risks of SCI.

As this class of vulnerability is specifically about processes executing side by side on the same CPU or memory chips of SCI, the risk of these vulnerabilities is being mitigated in CIP-005-8 by either:

- Declaring the VCAs that share CPU or memory or are within the same ESP with a BCS as associated PCAs which will require they meet the security requirements (high water marking) that include 'associated PCAs'; or
- Configuring the virtualization infrastructure to place VCAs of differing impact or trust levels into differing ESPs and configuring affinity controls to these zones such that hypervisors do not allow workloads in these differing zones to simultaneously exist or execute on the same hypervisor.

Assets with Multiple Classifications (PCA, EACMS, Intermediate System, SCI, etc.)

The definitions created in support of the CIP Standards have historically included overlap. In this current version of CIP-005-8, the definition of PCA is updated with conforming changes that include VCAs that share CPU or memory with a BCS. Additional definitions such as SCI and VCA will add to the possibility of additional instances of assets or systems meeting multiple definitions, such as SCI that are also EACMS.

These definitions are used in both the Applicable Systems column as well as within the requirement language. The fact that one asset or system may have multiple classifications does not pose a significant challenge as long as the Responsible Entity ensures that all requirements that pertain to ANY of the classifications are applied. In other words, if an asset or system meets both the SCI and the EACMS definition, requirements that apply to either definition are applicable.

Requirement R1

Rationale

Requirement R1 requires implementation of an ESP between systems of different impact levels such that only necessary communication is allowed between them. However, there are other network security models available now (such as zero trust) that can accomplish this security objective that are not network perimeter-based and control these communications end-to-end at a session level. However, the network border-based ESP model continues unchanged as CIP-005-8 Requirement R1 moves to an objective-based requirement that the network border-based model continues to meet while allowing for other models.

Requirement R1 Part 1.1:

Rationale

This requirement part is a combination of the first three requirement parts (1.1-1.3) in the former CIP-005-7 into one security objective. Virtualization technologies introduce multiple additional methods to isolate systems and communications beyond the network perimeter-based model. This requirement part is now objective-based and does not prescribe one method of controlling communications to Applicable Systems.

By moving to an objective-based requirement, network border-based models still meet the objective but it allows for other models such as zero trust architectures. Such models are not based on network perimeter-based security that controls communications at a network boundary. Communications are authorized by policy enforcement points throughout the infrastructure. In this model, network security is less topology-based and more policy-based and is used to protect communication at a very granular level (an individual system or even process or resource level).

While zero-trust architectures are an emerging model, the objective-based requirement also allows for hybrid models that are various combinations of network border-based and zero trust architectures. As technology changes, this requirement is flexible as to how the objective is met. The ESP definition has been broadened as well to accommodate models that create a security perimeter, but not necessarily by implementing a network border-based perimeter.

The requirement part maintains the core security objective of permitting only needed communications and denying all others; it simply no longer prescribes that this must be implemented at a Cyber Asset interface on the network border (an EAP). However, by not prescribing the location it could allow for a firewall built into the host BCS itself as the location where this access control is implemented. Examples are a server running a Windows OS with the in-built Windows firewall, or a Linux server with an IPTABLES firewall, that are providing the only control of the communications to and from a system connected to a public network. In these instances, the management plane of the host is also the management plane of the network security control. The SDT's intent is a host-based firewall (see RFC 7288[1] for a discussion of host-based firewalls) does not have a sufficient level of isolation from the system it is protecting to meet this requirement. A compromise of the OS is a compromise of the network communications security control as well. Therefore, the SDT has addressed this with the statement in the requirement "*Host-based firewalls (that only protect the host on which they reside) are not a sufficient control to meet this requirement*." This does not prescribe a physically separate control. A virtual firewall running as a separate VCA on the same SCI would be sufficient, as would technology such as privileged introspection within the hypervisor; these controls are isolated from the host being protected. The intent of this Requirement Part is to control the 'reachability' of the Applicable Systems; filtering network communications *before* they reach the Applicable Systems and their OS, not as part of it. This is not to discourage the use of integrated host-based firewalls to further filter network traffic to a host, it just cannot be the ESP for the purposes of this requirement. For example, host based firewalls can be used for further system hardening as part of CIP-007 R1, but not as the ESP for CIP-005 R1.

---

[1] https://datatracker.ietf.org/doc/html/rfc7288

The Requirement Part brings to medium and high impact BCS the exclusion of communications between intelligent electronic devices (i.e., digital relays) that use routable communication protocols for time-sensitive protection or control functions. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by inserting an ESP and its controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles (sub-second response times) to protect BES assets. The SDT intent is a Responsible Entity using this technology is not expected to implement the electronic access controls in a situation where it would prohibit the proper function in the proper timeframe.

Requirement R1 Part 1.2:

Rationale

The SDT is proposing a new Requirement, CIP-005-8 Requirement R1, Part 1.2. The purpose of this requirement is to permit only needed communications to and from the Management Interfaces, denying all other communications, of the systems that are providing the protection of BES Cyber Systems in part 1.1; namely SCI that is independently identified (not a part of an “all-in” scenario and thus is isolating systems of different impact levels from each other) and EACMS that are enforcing an ESP. As these are vital controls to performing the isolation/segmentation between systems of differing impact levels, the access to the Management Interface whereby these controls could be compromised is to be protected.

Requirement R1 Part 1.3:

Rationale

As the same technologies used in on-premise virtualization are used by cloud vendors hosting systems from many different customers, the methods used to separate the management plane from the data plane developed quickly as systems moving to the cloud increased. For a cloud-based hosting facility to be successful, the tenants must share hardware resources (SCI as defined here) but have no ability to access or modify other tenants or their configuration. Cloud technology was forced to enhance existing methods and develop new methods to accomplish this separation. SCI presents the same issue for in-house (on-premise) virtualization environments to prevent users of various systems hosted on the SCI from affecting each other or the SCI’s configuration. CIP-005-8 Requirement R1 Part 1.3 addresses this risk within the CIP standards.

The SDT is proposing this new Requirement R1, Part 1.3 that applies to SCI that is independently identified (not a part of an “all-in” scenario and thus is isolating systems of different impact levels from each other). As virtualized servers, networks, switches, firewalls, and storage are logical constructs, controlling communications to the Management Interfaces of these systems becomes imperative. Communication with the Management Interfaces can allow users to create, modify, or delete objects or entire infrastructures, or move objects from one network to another. Therefore, administrative level or “management access” to the SCI is critical to the security and reliability of the hosted systems. By isolating the Management Interfaces of these devices from the larger audience of users that can communicate with the hosted tenant systems, the attack surface of the SCI is reduced to the group of users with administrative access. The intent is users of a BCS hosted on an SCI that is identified independently and hosting other VCAs of differing impact levels should be prevented from having any access to the Management Interface of the underlying SCI. For example, a user accessing a low impact BCS on SCI should have no ability to pivot from that system to the Management Interface and thus impact a higher impact BCS.

This new Requirement part therefore requires the denial of network communications to the Management Interfaces of SCI that is independently identified (not a part of an “all-in” scenario and thus is isolating systems of different impact levels from each other) from the hosted BCS VCA's on the SCI. It does not preclude a separate VCA that hosts the SCI Management Interface from being used to manage the SCI as that is not an applicable system from part 1.1, however it must still meet requirement part 1.2 as well as part 1.3. A separate VCA hosting only a Management Interface can be allowed necessary access from part 1.2 for administrative users, but all access from any hosted BCS must be denied per part 1.3.

Requirement R1 Part 1.4:

Rationale

Requirement R1 Part 1.4 was written to address the issue of "Super ESPs" with high or medium impact BCS at Control Centers that extend a single ESP beyond one PSP. This often applies to virtualized Control Center environments that implement network adjacency to allow workloads to automatically move from one physical location to another to increase BCS resiliency between primary and backup Control Centers.

In summary, Requirement 1 Part 1.4 within CIP-005-8 requires that data traversing communication links between the two PSPs be protected to preserve its integrity and confidentiality. This new requirement part works in conjunction with the new 4.2.3.3 exemption in the CIP standards that exempts the Cyber Systems associated with such communication links since the data is required to be protected per this requirement. Also, the requirement part that formerly was CIP-006-6, Requirement 1, Part 1.10 has been removed from CIP-006 and incorporated into this new 1.4 requirement part. This consolidates the protections of an ESP and its components that extend outside of a PSP into one requirement part within one standard.

Communications equipment associated with communications links (e.g., equipment belonging to carriers) is exempted from the CIP standards with the 4.2.3.2 exemption, however that only applies to equipment between discrete ESPs. However, in this extended ESP situation where a single ESP spans different sites or PSPs, that exemption does not apply and the potential exists for data to traverse a connection that uses third-party communications equipment that is unprotected inside an ESP. The SDT chose to create Requirement R1 Part 1.4 to enforce confidentiality and integrity controls (such as encryption) on the data that traverses PSPs that is within the same ESP that works in conjunction with the new 4.2.3.3 exemption. In this case where communication equipment is used to extend a single ESP to more than one PSP, the confidentiality and integrity controls required in CIP-005-8 Requirement R1 Part 1.4 isolate any protected data from access through the communications equipment.

This Requirement Part applies to the data that traverses between PSPs. The SDT also combined CIP-006-6 Requirement R1 Part 1.10) into this Requirement Part to incorporate cabling and non-programmable communication components that are not protected within a PSP with the intent to protect data moving across the state as well as data traversing cabling that crosses the hall outside of the PSP. This consolidates these two requirements on protecting an ESP that spans differing PSPs into one requirement. The requirement language specifically exempts the data that falls under CIP-012 Requirements in order to avoid the potential for double jeopardy as well as the time-sensitive protection or control functions as described in CIP-005-8 Requirement R1 Part 1.1 above.

Requirement R1 Part 1.5:

Rationale

The SDT included "SCI identified independently supporting an Applicable System above" to the scope of the requirement part to ensure that controls regarding Dial-up Connectivity are applicable to SCI as well.

Requirement R1 Part 1.6:

Rationale

The SDT made changes to specify that the known or suspected malicious communication detection is for Internet Protocol (IP) based traffic that enters or leaves the required ESP. Products available to implement this malicious communication detection are usually based on IP traffic (as defined in RFC 791 and upon which TCP and UDP reside).

Requirement R2:

General Considerations for Requirement R2.

External Routable Connectivity (ERC) and Interactive Remote Access (IRA)

The ERC and IRA definitions are changing substantively in order to:

1. Incorporate new models such as Zero Trust where a security perimeter is not necessarily a network perimeter and ESP's become very granular based on policies that can be established at "people to resource" levels rather than IP address levels.
2. Recognize those CIP Systems that are of an increased risk due to their "reachability" via ERC and that have IRA available to them even if they are serial-only, non-routable devices.
3. Continue to limit scope of requirement parts to those locations that have a high enough level of remote connectivity to support the requirement. Locations that have connectivity such as non-routable serial leased circuits should not have to increase their level of remote connectivity and attack surface to meet security requirements.

One issue from the V5TAG transfer document in the SDT's scope is that of a BCA that only speaks non-routable protocols over a serial port. These BCAs are not connected to a network with a routable protocol themselves and therefore can be considered to not be within an ESP and thus not have ERC or IRA. However, these BCAs can have interactive user access using those serial connections. The SDT's intent is to clarify that IRA can occur to a device with only a serial, non-routable connection through subsequent IP-to-serial conversions and be subject to CIP-005-8 Requirement R2. For example, the intent is to clearly cover situations where a serial-only, non-routable BCA, such as a digital relay in a substation, has its serial communication from a 'console port' converted to IP or other routable protocols thus allowing IRA from users outside the substation to use a routable protocol to interact with the serial device and to require the CIP-005-8 Requirement R2 protection for that IRA.

In modifying the Intermediate Systems definitions, the SDT removed related requirement-style language ("The Intermediate System must not be located inside the Electronic Security Perimeter"). The SDT clarified the objective in CIP-005-8 Requirement R2 that all IRA must be *through* an Intermediate System and added Requirement Part 2.6.2 that addresses the location of the Intermediate System through an objective-based requirement.

See the "CIP Definitions and Exemptions Technical Rationale" document for further explanation of the changes to the R2 related definitions.

The scoping of R2 has been clarified to "all IRA and vendor remote access" and the applicability of several Requirement Parts was updated for virtualized environments to include SCI identified independently.

Requirement R2 Part 2.1:

Rationale

The Applicable Systems section of this requirement was updated to include SCI identified independently (SCI identified in the "all-in" scenario from CIP-002 is already included as part of the BCS). This was done to ensure that the same safeguards for remote access methods and technologies exist for the applicable SCI as for the high and medium impact BCS and associated PCA being hosted on that SCI. Backwards compatibility with CIP-005-7 is maintained for entities that do not currently use SCI.

The inclusion of the SCI is intended to target the Management Interfaces (included in SCI definition) of the associated SCI. This is to ensure that the management of the SCI being used to support BCS is also protected in an equivalent manner.

The SDT has added to the scope of this Requirement Part 2.1 any EACMS that enforces the ESP for Applicable Systems in Part 1.1. The intent is to require IRA protections (Intermediate System, multi-factor authentication, etc.) for those users who are managing an EACMS that enforces an ESP, such as firewalls, policy enforcement points, or network switches with ACLs or VLANs that enforce an ESP. The intent is that such remote access from users that is 'to' (not 'through') the EACMS to configure the ESP requires the IRA protections.

The requirement language itself was simplified. Note the definitions of IRA and Intermediate System have been updated. Please note that the definition of IRA was changed to include serial communications connections. This change maintains backwards compatibility with CIP-005-7 except where serial connectivity is being used for IRA.

The required location of an Intermediate System was within the definition previously. The definition of Intermediate System has been simplified and the requirement as to its location is now within the requirement itself (Part 2.6.2) rather than within the definition.

Requirement R2 Part 2.2:

Rationale

The Applicable Systems was changed to "Intermediate Systems used to access Applicable Systems of Part 2.1". This change better reflects that this requirement is associated with the Intermediate System itself.

The requirement was changed from a specific technical based requirement for encryption to an objective based requirement to protect confidentiality and integrity of the IRA session between the Intermediate System and the remote client. The proposed language of this requirement accounts for the possibility that other equally effective methods could be developed and deployed. This objective also keeps methods from being used that are merely obfuscation methods (XOR, ROT13, etc.) or deprecated encryption methods (DES with 56-bit keys) that no longer actually protect the confidentiality and integrity of the IRA session.

The changed requirement is backwards compatible with the CIP-005-7 except where outdated encryption methods have been used.

Requirement R2 Part 2.3:

Rationale

The Applicable Systems was changed to "Intermediate Systems used to access Applicable Systems of Part 2.1". This change better reflects that this requirement is associated with the Intermediate System itself. This change also clarifies where the requirement for multifactor authentication should be applied (multi-factor authentication to the Intermediate System).

The changed requirement is backwards compatible with the CIP-005-7 except where serial connection-based IRA is being utilized.

Requirement R2 Part 2.4 – 2.5:

Rationale

The Applicable Systems section of this requirement was updated to include SCI identified independently (SCI identified in the “all-in” scenario from CIP-002 is already included as part of the BCS), in instances where vendor remote access is allowed to the SCI (including its Management Interfaces). The Applicable Systems were also modified such that only those with vendor remote access are in scope and thus need to have one or more methods for CIP-005-8 Requirement R2 Parts 2.4 and 2.5.

The requirements themselves have not been changed. Note that the requirement includes both vendor-based IRA and system-to-system access.

Requirement R2 Part 2.6:

Rationale

This is a new requirement that applies to Intermediate Systems that are required by CIP-005-8 Requirement R2 Part 2.1. The intent of this new requirement is to further protect the BCS from the Intermediate System by reducing the attack surface between the two. Intermediate Systems have an externally accessible interface that may be used by external parties such as vendors or entity support staff using IRA across an Internet connection to support a remote site. Since Intermediate Systems by nature provide IRA from a less-trusted network, a degree of separation from the higher-trust systems they are protecting is necessary in case the Intermediate System is compromised. Previously, this risk was addressed not in an actual requirement but within the glossary definition of Intermediate System (“…must not be located inside the ESP”). The SDT has removed this from the definition and included a security objective in CIP-005-8 Requirement R2 Part 2.6.2 to permit only needed and controlled communications between the Intermediate System and the Applicable Systems it is providing IRA to.

In order to mitigate the risk of a compromised virtualized Intermediate System (VCA) hosted on SCI, Requirement CIP-005-8 Requirement R2 Part 2.6.1 restricts CPU and memory sharing on SCI to only its associated SCI and other Intermediate Systems. In summary, CIP-005-8 Requirement R2 Part 2.6.1 is intended to mitigate the risk associated with “side channel” based attack vectors where it could be possible to compromise the Intermediate System VCA from an external source and then subsequently access other CIP System VCAs running on the same hypervisor within the SCI.

Requirement R3

Rationale

The Applicable Systems section of CIP-005-8 Requirement R3 was updated to include “SCI identified independently supporting an Applicable System above” to ensure the same safeguards for vendor-initiated remote connections exist for the applicable SCI. Backwards compatibility with CIP-005-7 is maintained for entities that do not currently use SCI.

Former Background Section from Reliability Standard CIP-005-7

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BCS and require a minimum level of organizational, operational and procedural controls to mitigate risk to BCS.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BCS. For example, a single training program could meet the requirements for training personnel across multiple BCS.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

Technical Rationale for Reliability Standard CIP-005-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team’s (SDT’s) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission’s Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The ESP serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of ‘Associated Protected Cyber Assets’ that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the ‘high water mark’).

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the “high water mark”) where the term “Protected Cyber Assets” is used. The CIP Cyber Security Standards accomplish the “high water mark” by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as “Protected Cyber Assets” of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are “Associated Protected Cyber Assets” of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually ‘command and control’ hosts on the Internet, or compromised ‘jump hosts’ within the Responsible Entity’s other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT’s intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT’s intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and ‘deny by default’ type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear ‘perimeter type’ security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions (“TFEs”) rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-

15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e. system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the “first line of defense within an Industry Control System (ICS) network environment”. The compromise of those devices that control access management could provide an outsider the “keys to the front door” of the ESP where BES Cyber Systems reside. An intruder holding the “keys to the front door” could use those “keys” to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[2].

NERC's final report on "*Cyber Security Supply Chain Risks*", states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks*" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

---

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an “Associated Protected Cyber Asset” of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually ‘command and control’ hosts on the Internet, or compromised ‘jump hosts’ within the Responsible Entity’s other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT’s intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity’s address space. The SDT’s intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and ‘deny by default’ type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear ‘perimeter type’ security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions (“TFEs”) rather than increased security.

As for dial-up connectivity, the Standard Drafting Team’s intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Physical Security of BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-006-7

June 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-006-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-006-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-006-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The SDT added the option (known as the "all-in" scenario) for entities to group SCI within a BCS it supports; Therefore, to enable CIP-006-7 for virtualization, the SDT added "SCI identified independently supporting an Applicable System above…" each of the Parts in Applicable Systems for Requirement R1 to account for the alternative option (See the CIP-002 Technical Rationale document for a description of the options for identifying SCI and reasons an entity may choose between the options.)

The SDT chose not to renumber Parts 1.1 – 1.3 of Requirement R1 due to the undue administrative impact to entity's documented programs caused by such renumbering. As a result, Part 1.1 through 1.3 remain constructed in an additive order as the impact or connectivity to said Applicable System increases. The list of Applicable Systems had become lengthy and confusing within this construct, so in an effort to bring clarity, the SDT was mindful to streamline the Applicable Systems through exclusionary references to other Parts. This approach assures the appropriate scoping is retained within this construct without creating double jeopardy, while bringing clarity and brevity to the Applicable Systems column for each Part. The results are as follows:

Applicable Systems:

Requirement R1 Part 1.1: the SDT added "SCI identified independently supporting an Applicable System above, not included in the Applicable Systems of Part 1.2 or Part 1.3"

Requirement R1 Part 1.2: the SDT added "SCI identified independently supporting an Applicable System above, not included in the Applicable Systems of Part 1.3"

Requirement R1 Part 1.3 – 1.9: the SDT added "SCI identified independently supporting an Applicable System above"

Per System Capability vs Technical Feasibility:

Requirement R1 Part 1.3: The SDT chose to remove the reliance on a Technical Feasibility Exception in favor of the updated term "per system capability." Rationale: The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception.

CIP Exceptional Circumstances (CEC):

The SDT also evaluated where CIP Exceptional Circumstances (CEC) should be included, and has added this provision to the following requirement parts:

Requirement R1 Part 1.8: Rationale: Responsible Entities may not be able to log entry of each individual with authorized unescorted physical access into each Physical Security Perimeter (PSP) if a facility that contains the PSP or Physical Access Control System is damaged or destroyed.

Requirement R1 Part 1.9: Rationale: Responsible Entities may not be able to retain access logs of entry of individuals into each PSP if a facility that contains the PSP or Physical Access Control System is damaged or destroyed.

Consolidation:

Requirement R1 Part 1.10: The SDT deleted Requirement R1 Part 1.10 from CIP-006-7 because it is incorporated into CIP-005-8 Requirement R1 Part 1.4.

Requirement R2 – Requirement R3

Rationale

The SDT added the option (known as the "all-in" scenario) for entities to group SCI within a BCS it supports; Therefore, to enable CIP-006-7 for virtualization, the SDT added "SCI identified independently supporting an Applicable System above" each of the Parts in Applicable Systems for Requirement R2 – Requirement R3 to account for the alternative option (See the CIP-002 Technical Rationale document for a description of the options for identifying SCI and reasons an entity may choose between the options.)

Requirement R1 Part 3.1: To accommodate for the variant construct of Applicable systems in Requirement R3 Part 3.1 specifically, the phrase “identified independently supporting” was used in each SCI bullet beneath “Physical Access Control Systems (PACS)” and “Locally mounted hardware or devices at the Physical Security Perimeter”.

Former Background Section from Reliability Standard CIP-006-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-006-6

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-006-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed “six-wall” boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

- Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the PSP.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more PSPs, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the “guard” has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity's BES Cyber Systems while not requiring controls to be implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the PSP to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the PSP. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a PSP (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any PSPs protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — System Security Management

Technical Rationale and Justification for Reliability Standard CIP-007-7

June 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-007-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-007-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-007-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale.pdf" for reference when reading the technical rationale that follows.

General Considerations
Requirement R1
General Considerations for Requirement R1

Independently identified Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-007-7 for virtualization, the SDT added SCI identified independently and related it to the BCS and associated Cyber Assets already listed in Applicable Systems. This approach keeps the SCI applicability parallel to each existing variant of medium impact BCS (i.e. Medium impact BCS vs. Medium impact BCS with External Routable Connectivity (ERC) vs. Medium impact BCS at Control Centers etc.)

Change Rationale Requirement R1:

The SDT has changed the name of the R1 table to “System Hardening” to more clearly reflect the security objective of the entries in the table which is to harden the applicable systems through limiting access to logical and physical ports, and to control where certain VCAs can instantiate through host affinity rules.

The SDT chose to include “SCI identified independently…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCAs.

Change Rationale Requirement R1 Part 1.1: Requirement R1 Part 1.1 adds the clarifier of Internet Protocol (IP) to the port references in order to ensure only those network accessible IP ports are within scope of this requirement. This was done in order to ensure ports such as those associated with non-IP network communications (such as with a SAN over Fiber Channel) do not fall within scope of the Requirement Part. Additionally, the option to rely on the service, if the IP port is not known, has been added to the Requirement Part.

The SDT chose to remove the reliance on a Technical Feasibility Exception in favor of the updated term “per system capability”. The SDT contends that the term still requires an entity to document the limit to the system’s capability with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception.

Change Rationale Requirement R1 Part 1.3:

Requirement R1 Part 1.3 is a new requirement intended to apply host affinity controls to SCI identified independently. The risk associated with an SCI identified independently is such that it may host non-CIP Systems, and therefore must be protected at a higher level than those SCI that are included within the BCS, EACMS or PACS that they support. This is one of the controls added for SCI identified independently that serves as an additional hardening control required due to this higher risk.

Requirement R2

Change Rationale Requirement R2:

The SDT chose to include "SCI identified independently…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCAs.

The SDT made conforming changes where necessary with Requirement R2 to remove reliance on the Cyber Asset term, choosing to reference the system instead.

Backward Compatibility

CIP-007-7 Requirement R2 retains backward compatibility for entities without SCI identified independently.

The SDT intends that entities take full advantage of their virtualization infrastructure in order to ease the overhead associated with patch management. While many of the entity's existing processes will remain the same, (such as those associated with tracking the source of security patches, evaluation of the applicability of available patches and mitigation plans for those applicable patches that cannot be installed) new or modified processes around the installation of patches can be used (for example, parent images, remediation VLANs, etc.)

Parent Images

One of the interesting nuances of virtualization is the concept of parent/child relationships.

Some VCAs utilize a "parent image" type methodology where the specific VCA software and operating system is merely a child instance of a parent image. In such cases, the application of security patches to the parent image also applies the same changes to any children of that image. As there may be many child instances, the administrative overhead associated with patching of those instances can be greatly reduced.

Dormant Instances

There are times when VCAs are not being used and are idle. Physical instances of the assets are always left up and running in order to receive applicable patches, software updates, configuration updates, etc.

Leveraging the built in virtualization features allows idle resources to be reassigned to tasks at hand without incurring additional overhead of tracking which dormant virtual instances require patching. Dormant virtual instances are just files with the saved state of the VCA. Dormant instances are not VCAs themselves nor Applicable Systems until they become active instances again.

Where a dormant virtual instance is also the child instance of a parent image, the application of security patches to the parent image will also make the same changes automatically when needed to any out of date dormant child virtual instances when they are restarted.

In most cases, a dormant virtual child instance is made active again on a remediation type network where any missing security patches (compared to the parent image) are automatically applied before it is placed back into active service.

Saved Images

Similar to dormant child images, saved child images or snapshots may be also used as functional backups for CIP-009 purposes in order to provide fast restoration and better availability. If an active VCA becomes corrupted, a saved image can be made active where the application of any missing security patches (compared to the parent image) can be automatically applied, through remediation, before being placed back into active service.

Requirement R3

Change Rationale Requirement R3:

The SDT chose to modify the name of the Table in R3 from Malicious Code Prevention to the term used by the National Institute of Standards & Technology (NIST), Malicious Code Protection, as that more accurately clarifies the security objective of protecting BCS from malicious code.

The SDT chose to include “SCI identified independently…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCAs.

Requirement R4

Change Rationale Requirement R4:

The SDT chose to include “SCI identified independently…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCAs.

Change Rationale Requirement R4 Part 4.1:

The SDT determined the entire structure of the “at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)” language could be simplified to “per system capability” since the Applicable Systems column clarifies what systems are included.

Additionally, the SDT chose to insert the word “security” as a clarifier to which events are to be logged.

Change Rationale Requirement R4 Part 4.2:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the “Cyber Asset” term, as well as the ambiguity that would have existed if the term “BES Cyber System” were left in place while the Applicability Column included SCI.

Change Rationale Requirement R4 Part 4.3:

The SDT also chose to remove the reliance on a Technical Feasibility Exception from Part 4.3 in favor of the updated term “per system capability”. The SDT contends that the term still requires an entity to document the limit to the system’s capability with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception.

Requirement R5

Change Rationale Requirement R5:

The SDT chose to include “SCI identified independently…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCAs.

Change Rationale Requirement R5 Parts 5.1, and 5.6 – 5.7:

The SDT chose to remove the reliance on Technical Feasibility Exception in favor of the updated term “per system capability”. The SDT contends that the term still requires an entity to document the limit to the system’s capability with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception.

Change Rationale Requirement R5 Part 5.5:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the “Cyber Asset” term, replacing it with a reference to the Applicable Systems.

Former Background Section from Reliability Standard CIP-007-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-007-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-007-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

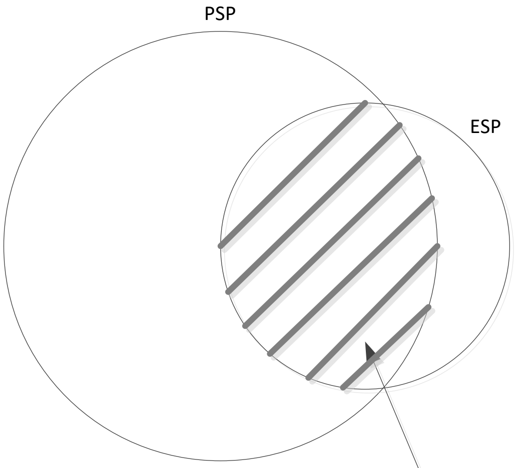
- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:

Location of Nonprogrammable Communication Components



Applicability of CIP-007-6 R1, Part 1.2 for Nonprogrammable Communication Components

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media (“transient devices”) in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms

- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement’s rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT
Cyber Security – Incident Reporting and Response Planning

Technical Rationale and Justification for Reliability Standard CIP-008-7

June 2021

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-008-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-008-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 – Requirement R4

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-008-6 to align incident reporting and response planning requirements with the virtualization changes.

The SDT added the option (known as the "all-in" scenario) for entities to group SCI within a BCS it supports; Therefore, to enable CIP-008-7 for virtualization, the SDT added "SCI identified independently supporting an Applicable System above" each of the Parts in Applicable Systems for Requirement R1 – Requirement R4 to account for the alternative option (See the CIP-002 Technical Rationale document for a description of the options for identifying SCI and reasons an entity may choose between the options.)

Requirement R4

Rationale

The Project 2016-02 SDT made updates to reflect the change from the National Cybersecurity and Communications integration Center (NCCIC) to its successor organization Cybersecurity & Infrastructure Security Agency (CISA), and deleted the superfluous footnote in favor of deference to the Requirement language, which already states, “or their successors”.

Former Background Section from Reliability Standard CIP-008-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

Medium Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

Technical Rationale for Reliability Standard CIP-008-6

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-6. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-008-6 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 19, 2018, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 848. In this Order FERC directed the North American Electric Reliability Corporation (NERC) to "develop and submit modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access and Control or Monitoring System (EACMS)." (Order 848, Paragraph 1)

In response to the directive in Order No. 848, the Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require Responsible Entities to implement methods augmenting the mandatory reporting of Cyber Security Incidents to include: "(1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report included specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT)." (Order 848, Paragraph 3)[1]

New and Modified Terms Used in NERC Reliability Standards

CIP-006-6 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms:

Cyber Security Incident

A malicious act or suspicious event that:

- *For a high or medium impact BES Cyber System, compromises, or attempts to compromise the, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or*
- *Disrupts, or attempts to disrupt, the operation of a BES Cyber System.*

In response to FERC Order 848, Paragraph 1, the SDT modified the Cyber Security Incident definition to include Electronic Access Control or Monitoring Systems (EACMS) associated with high or medium impact BES Cyber Systems, in response to the Order.

---

[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

The addition of high and medium impact BES Cyber Systems considers the potential unintended consequences with the use of the existing definition in CIP-003-7. It also provides clarity that only low impact BES Cyber Systems are included within the definition. ESP or EACMs that may be defined by an entity for low impact BES Cyber Systems are not part of the definition.

An attempt to disrupt the operation of a BES Cyber System is meant to include, among other things, a compromise of a single BES Cyber Asset within a BES Cyber System. For example, malware discovered on a BES Cyber Asset is an attempt to disrupt the operation of that BES Cyber System.

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:

- *A BES Cyber System that performs one or more reliability tasks of a functional entity;*
- *An Electronic Security Perimeter of a high or medium impact BES Cyber System; or*
- *An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber Systems.*

The Reportable Cyber Security Incident definition was modified to comply with FERC Order 848. In response to Paragraph 54 of the Order, the SDT modified the definition to include incidents that compromised or disrupted an ESP or an EACMS. The team also added the qualifying clause for “A BES Cyber System that performs one or more reliability tasks of a functional entity” to clarify what was compromised or disrupted, thus not extending the scope to Protected Cyber Assets (PCAs). In response to comments, the SDT left the entire definition of BES Cyber system in Reportable Cyber Security Incident to provide clarity.

It is also important to understand the relationship between the two definitions, the requirement language, and how they work in concert to classify events and conditions at varied levels of significance as the Registered Entity executes its process and applies its defined criteria to determine if reporting is required.

Electronic Access Control or Monitoring Systems (EACMS)

The drafting team spent significant time discussing this topic among its members, through industry outreach, and with FERC staff. The team believes by not specifically referencing the five functions in Order 848, we have reduced complexity and made compliance with the Standard achievable. The drafting team asserts that the five functions are equivalent to the current definition of EACMS in the NERC Glossary of Terms. If entities have questions about application of the EACMS definition, the drafting team advises entities to discuss those questions directly with NERC.

Requirements R1, R2, and R3

General Considerations for Requirement R1, Requirement R2, and Requirement R3

FERC Order 848, Paragraph 1, directs modifications to Reliability Standards to require reporting of incidents that compromise, or attempt to compromise a responsible entity's ESP or associated EACMS. The intent of the SDT was to minimize the changes within CIP-008 and address the required modifications. To do this, the SDT added "and their associated EACMS" to the "Applicable Systems" column for Requirements R1, R2, and R3.

To add clarity to "attempts to compromise," the drafting team created Part 1.2.1 to require entities to establish and document their process to include criteria to evaluate and define attempts to compromise. This requirement maps to Requirement 4 Part 4.2, which requires entities to use that entity-defined process for determining which incidents entities must report.

The use of the language describing Cyber Security Incident(s) as being "an attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the 'Applicable Systems'" column for the Part is meant to clarify which Cyber Assets are in scope for attempts to compromise reporting by entities. This language is used throughout the standard.

Moving Parts of Requirement R1 to Requirement R4

To minimize the changes to Requirement R1, the SDT created Requirement R4 and consolidated all the CIP-008-6 reporting requirements. The SDT deleted Requirement R1 Part 1.2 reporting requirements from CIP-008-5, and moved them to Requirement R4 for this purpose.

Inclusion of "Successor Organizations" throughout the Requirement Parts

The SDT recognizes that organizations are constantly evolving to meet emerging needs, and may re-organize or change their names over time. The ICS-CERT has completed its name change to the National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems. The E-ISAC previously re-branded its name and may again in the future. By following Requirement R4 references to E-ISAC and NCCIC with "or their successors" the SDT is ensuring that Requirement R4 can be implemented even if the names of E-ISAC and NCCIC change or a different agency takes over their current roles.

Requirement R4

General Considerations for Requirement R4

Requirement R4 is a new requirement focused on mandatory reporting of Reportable Cyber Security Incidents and includes attempts to compromise systems in the "Applicable Systems" column. Previously, CIP-008-5 defined reporting requirements for Reportable Cyber Security Requirements (Requirement R1 Part 1.2) only.

Required Reportable Incident Attributes

Requirement R4.1 specifies that initial notifications and updates must include three attributes: 1) functional impact, 2) attack vector used, and 3) level of intrusion achieved or attempted. These attributes are taken directly from the Order. (FERC Order No. 848, paragraph 89).

The SDT understands that some or all of these attributes may be unknown at time of initial notification. To account for this scenario the SDT included "to the extent known" in the requirement language. There is an expectation that update reporting will be done as new information is determined or unknown attributes become known by the entity. There could be cases, due to operational need, that all the attributes may never be known, if this case presents itself that information should be reported.

Methods for Submitting Notifications

Requirement R4 Part 4.2 allows responsible entities to submit notification using any method supported by E-ISAC and NCCIC. The SDT did not prescribe a particular reporting method or format to allow responsible entities' personnel to focus on incident response itself and not the method or format of reporting. It is important to note the report must contain the three attributes required in Requirement R4 Part 4.1 as they are known, regardless of reporting method or format.

Notification Timing

Requirement R4 Part 4.2 specifies two timelines for initial notification submission; one hour for Reportable Cyber Security Incidents; and end of next calendar day for attempts to compromise systems in the "Applicable Systems" column. Paragraph 3 of FERC Order No 848 directly states that reporting deadlines must be established. Paragraph 89 further states that "timelines that are commensurate with the adverse impact to the BES that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES."

- *Reportable Cyber Security Incidents* – The SDT wrote Requirement R4 Part R4.2 to use a one hour deadline for reporting of these events because incidents in this category include successful compromise of ESP(s), EACMS, or BES Cyber System(s). One hour is referenced directly in FERC Order No 848 paragraph 89 and is also the current reporting requirement in CIP-008-5.
- *Cyber Security Incident that was an attempt to compromise one or more systems identified in the "Applicable Systems" column* - Due to the lower severity of these unsuccessful attempts at compromising ESP(s), EACMS, or BES Cyber System(s), the SDT proposed a longer reporting timeframe. The intent behind the decision to add "By the end of the next calendar day" (11:59 pm local time) was to give responsible entities additional time to gather facts prior to notifications for the less severe attempts to compromise Applicable Systems. It is important to note that compliance timing begins with the entity's determination that attempt to compromise meets the process they defined in Requirement R1 Part 1.2.1.

The SDT understands initial notification may not have all the details when first submitted. It is expected, however, that information that has been determined is reported within the notification deadlines. Additionally, it is important to note the wording in Requirement R4 Part 4.2. The "compliance clock" for the report timing begins when the Responsible Entity executes its process from Requirement R1 Part 1.2.1 and a determination has been made that the type of incident which has occurred qualifies as reportable.

Technical rationale taken from the Guidelines and Technical Basis (GTB) CIP-008-5 Requirement 1 provides additional justification for the SDT to maintain the one hour timeframe for Reportable Cyber Security Incidents.

> *"The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."*

In 2007, the Electricity Information Sharing and Analysis Center (E-ISAC) was known as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Its voluntary procedures required the reporting of a cyber-incident within one hour of an incident. CIP-008-1 required entities to report to the ES-ISAC.

In FERC Order No. 706[2] (July 18, 2008), the Commission concluded that the one-hour reporting limit was reasonable [P 663]. The Commission further stated that it was leaving the details to NERC, but it wanted the reporting timeframe to run from the "**discovery**" of the incident by the entity, and not the actual **"occurrence"** of the incident [P 664].

CIP-008-2 and CIP-008-3 were silent regarding the required timeframe for reporting, but it was specifically addressed in CIP-008-5. In the October 26, 2012, redlined version of CIP-008-5, the proposed language for initial notification originally specified "one hour from **identification**" of an incident. This aligned with the Commission's decision in Order No. 706, for the clock to start with the discovery of an incident. However, the Standard Drafting Team changed "one hour from identification" to "one hour from the **determination** of a Reportable Cyber Security Incident". This language was subsequently approved and incorporated into CIP-008-5.

These changes, from "occurrence" to "discovery" to "determination," provide the additional time needed for the entity to apply its specifically created process(es) for determining whether a Cyber Security Incident rises to the level of required reporting. This determination timeframe may include a preliminary investigation of the incident which will provide useful information to other entities to help defend against similar attacks.

---

[2] 2008, Federal Energy Regulatory Commission, Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706.

Notification Updates

Requirement R4 Part 4.3 requires that Responsible Entities submit updates for the required attributes upon determination of new or changed attribute information, if any. The SDT added this language to provide entities sufficient time to determine attribute information, which may be unknown at the time of initial notification, and which may change as more information is gathered. The intent of Requirement R4 Part 4.3 is to provide a method for Responsible Entities to report new information over time as their investigations progress. NOTE: The SDT does not intend updates specified in Requirement R4. Part 4.3 to expose responsible entities to potential violations if, for example, initial and updated notification on the same attribute have different information. This is expected since knowledge of attributes may change as investigations proceed. Rather, the intent of Requirement R4 Part 4.3 is to have a mechanism to report incident information to E-ISAC and NCCIC (and thereby industry) upon determination of each required attribute.

The intent is that the entity report what is known and document the reason not all attributes could become known and ultimately be reported in conditions where, e.g. a Cyber Asset was restored completely, removing all forensic evidence in order to restore operations, which caused the entity to conclude its investigation without having a complete knowledge of the three required attributes.

The SDT asserts that nothing included in the new reporting Requirement R4, precludes the entity from continuing to provide any voluntary sharing they may already be conducting today.

Technical Rationale for Reliability Standard CIP-008-5

This section contains the Guidelines and Technical basis as a “cut and paste” from CIP-008-5 standard to preserve any historical references.

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for Reportable Cyber Security Incidents.

Entities may use an actual response to a Reportable Cyber Security Incident as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise.

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for Reportable Cyber Security Incidents. There are several examples of specific types of evidence listed in the measure.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

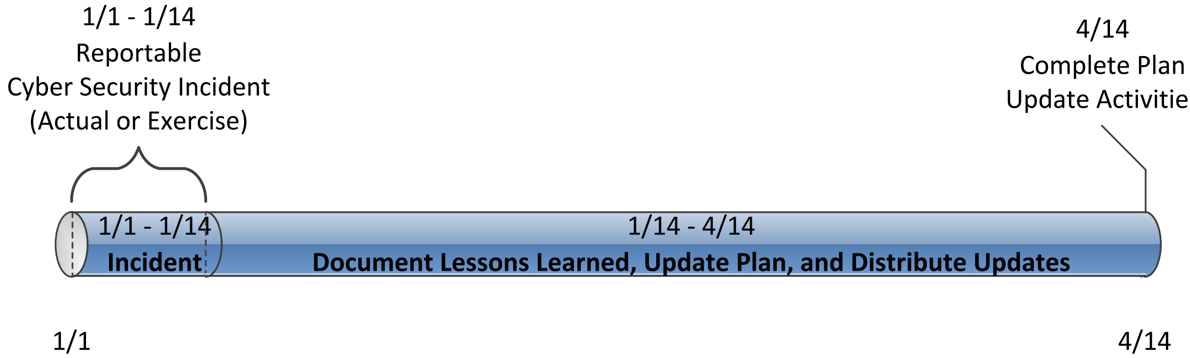
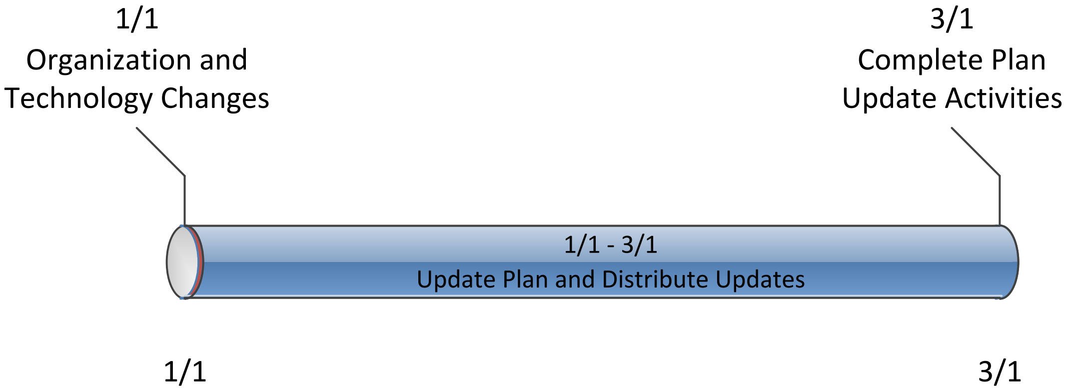


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals.

Figure 2: Timeline for Plan Changes in 3.2



Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)
"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)
Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)
Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)
Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)
Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)
Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)
Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Recovery Plans for BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-009-7

June 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-009-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-009-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-009-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 – Requirement R3

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-009-7 to align recovery planning requirements with the virtualization changes.

The SDT added the option (known as the “all-in” scenario) for entities to group SCI within a BCS it supports. Therefore, to enable CIP-009-7 for virtualization, the SDT added “SCI identified independently supporting an Applicable System above” each of the Parts in Applicable Systems for Requirement R1 – Requirement R3 to account for the alternative option (See the CIP-002 Technical Rationale document for a description of the options for identifying SCI and reasons an entity may choose between the options.) Additionally, the use of the term BES Cyber System has been replaced with “Applicable System” within the requirement language of Requirement R1 Part 1.3 and Requirement R2 Part 2.2 to align the requirement with the applicability for each Requirement Part.

Former Background Section from Reliability Standard CIP-009-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.

An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-009-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-009-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, “A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures.”

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, “[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and ‘boots on the ground’ response (e.g., firefighters decontaminating mock victims).”

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

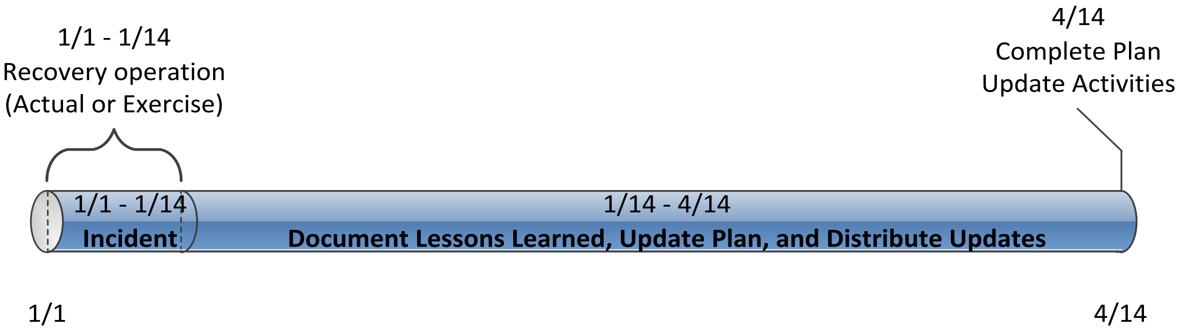


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

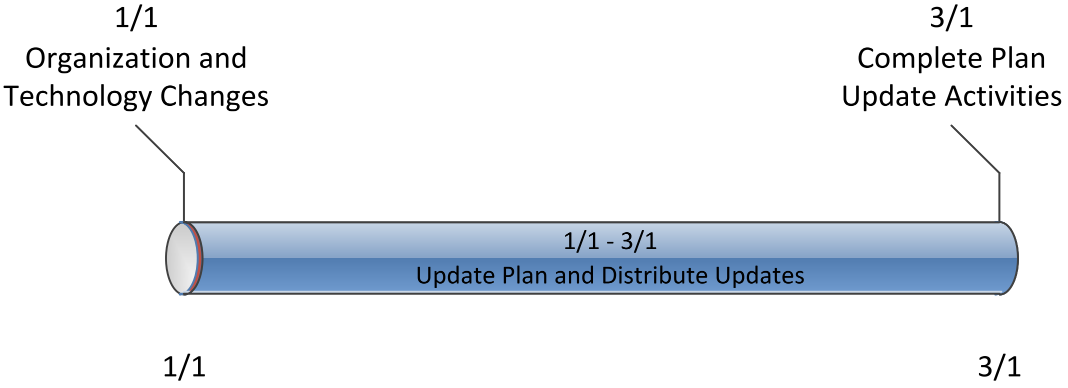


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-5

June 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-010-5

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-5. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-010-5 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

The proposed changes in CIP-010-5 from the Project 2016-02 SDT concern the use of several facets of virtualization technologies. Virtualization allows for such technologies as new controls for Shared Cyber Infrastructure (SCI), remediation VLANs, parent/child images, and dormant virtual machines (VMs). Enabling and clarifying the use of these technologies is the basis of the proposed changes in CIP-010-5. A general introduction to each of these technologies follows.

Shared Cyber Infrastructure (SCI)

Virtualization abstracts the software layers (the OS and applications) from the underlying hardware to allow for hardware to be shared among several Virtual Cyber Assets (VCAs). Hypervisors include security controls to keep these workloads logically isolated from one another and their requirements are within other CIP standards such as CIP-005. However, with any type of shared infrastructure, the need for change management requirements is elevated for those security controls that allow for the 'shared' in SCI. Such controls are added to the change management requirements in CIP-010-5.

Remediation VLAN

Remediation VLAN is a term used to describe a logical network segment in which a computing device can be isolated from other production systems and examined to ensure the integrity and validity of the configuration and software installed on the device before it is permitted to transition to the production network segment.

This examination is policy driven, meaning that the administrator is able to configure what the minimum requirements are for admission to the production network. Examples of this might be minimum operating system patch levels or recent anti-virus definitions.

If during the examination of the computing device, it is found to not comply with the requirements defined in the policy, an administrator may intervene to manually remediate the deficiencies, or the system which was used to examine the device may communicate the deficiencies to the device with instructions on how to remediate itself in an automated fashion. After the remediation actions are taken, the computing device can request to be re-examined and if the requirements dictated by the policy are now met, it will be permitted access to the production network segment.

Parent/Child Images

When a VCA is ‘powered on’, it instantiates (“boots”) from a disk image file. Since the boot ‘disk’ is a file and not physical disk, many individual VCAs can use the same “parent” image as the basis for their own “child” image. Among other things, this allows for patching of an OS to occur to a parent image and the child images then pick up that patched image upon their next instantiation.

Dormant VMs

A VCA that is not instantiated (i.e. not ‘booted up’ and executing) is a dormant VM. It exists not as a traditional cyber asset, but simply as a file. VCA’s can be created for specialized purposes such as to run troubleshooting tools and only be instantiated when needed with long periods of times in between, during which they exist as a file. They are not up and running and on the network where they are managed and patched on a regular basis. However, these can go hand-in-hand with remediation VLANs which would bring them up to date as soon as they do instantiate but before they have access to any other systems.

General Considerations

SCI is mutually exclusive from Cyber Assets (CA) by definition. To enable CIP-010-5 for virtualization, the SDT evaluated the existing Applicable Systems and added SCI that supports each applicable BCS variant and associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), or (Protected Cyber Assets (PCAs) already listed in Applicable Systems. This approach keeps the SCI applicability parallel to each existing variant of medium impact BCS (i.e. Medium Impact BCS vs. Medium Impact BCS with External Routable Connectivity (ERC) vs. Medium Impact BCS at Control Centers etc.).

Based on the updates to CIP-002 proposed with this version of CIP-010-5, SCI can be handled in two ways. A Registered Entity can choose to include the SCI within the CIP System it supports, and therefore treat it as a part of that system and apply all applicable CIP Requirements that apply to the CIP System it is included within. Alternatively, the SCI can be identified independently, which adds the flexibility to host multiple CIP Systems, even of differing impact ratings, however because of this flexibility, the SCI identified independently has additional controls which apply only to the SCI, and not the CIP Systems it supports.

Requirement R1

General Considerations for Requirement R1

In prior versions, CIP-010 Requirement R1 has required developing a baseline configuration that consisted of five (5) items (OS, installed and custom software, ports, patches). The baseline configuration was then used in the remainder of Requirement R1 and R2 as the basis of change management including testing. At a high level, the current Requirement Part 1.1 was to develop a baseline config, Requirement R1 Part 1.2 was to authorize and document changes to the items in the baseline config, and Requirement R1 Part 1.3 was to update the baseline config within a specific timeframe of a change. This tended to focus the requirement on documenting past changes.

In CIP-010-5, as the SDT considered the more policy-based and automated virtualization technologies discussed in the previous section, the SDT determined to change the focus of Requirement R1 towards a security objective of authorizing upcoming changes rather than maintaining a baseline configuration. Maintaining baseline configurations remains one possible "how", but it is no longer the only prescribed "how." The phrase "baseline configuration" has been removed from CIP-010-5 as a result. This maintains compatibility with current state but allows flexibility for virtualization technologies. This also ensures the focus is not on documenting past changes but the authorization of current or future changes, thus making the requirement forward looking with a clearer security objective.

Rationale for Requirement R1 Part 1.1

The original CIP-010 Requirement R1 Part 1.1 included establishing a baseline configuration for assets that included a set of items that would then be monitored for changes in the remaining parts of Requirement R1. This process is continued in the replacement for Requirement R1 and its Parts, however the documentation requirement (CIP-010-4 Requirement R1 Part 1.1) is no longer focused on a documentation only activity. While a Responsible Entity can benefit from documenting the configuration or the various elements of Requirement R1 Part 1.1 (1.1.1 – 1.1.4) this is no longer a requirement on its own. Maintaining this documentation is now one possible control to use to ensure changes to those elements are managed as required.

Additional changes were introduced to allow for or enable further use of virtualization. Specifically, the addition of "images used to derive operating systems or firmware" found in Requirement Part 1.1.1 is accounting for the concept of virtualized systems based on a "parent image." These images may be updated separately from a derived virtual machine and become active as soon as the virtual machine is rebooted. In this case, changes to this parent image must follow the management requirements found in Requirement R1.

Dormant VMs was another change with the current focus on baseline documentation, since the dormant VM is really just a file on disk, and as such cannot impact the BES until it is instantiated, at which time it must be compliant with the requirement. In many cases dormant VMs are patched to current prior to being added to the "production" network. By focusing the Part 1.1. requirement on the authorization to change as opposed to documentation of a current configuration, the challenge is mitigated. The Registered Entity must still know what is current, in order to know they must authorize a change, but the obligation to keep documentation up to date for a dormant VM is removed.

Additionally, the SDT noted that with the shift from a documentation requirement to a change authorization requirement, the bulk of the changes to the OS and installed software will be security patches. In this light, the inclusion of installed security patches in the list of items to authorize changes to would be duplicative, and provide no security benefit. Security Patches will be authorized through the authorization to change the OS or installed software through the installation of a security patch.

Rationale for Requirement R1 Part 1.2

Specific configuration items are included which apply only to SCI. These exist because the SDT determined that SCI that hosts BCS or associated EACMS, PACS or PCAs have controls that apply to specific configuration items relevant only to SCI.

Requirement R1 Part 1.2 is a new addition in order to require the authorization of changes to SCI configuration as it pertains to other required security controls (such as in CIP-005). The sharing of infrastructure puts a premium on the management of the security controls that enforce the logical isolation between tenants and the services the SCI itself uses. These areas that should fall under a CIP-010 management program are contained in Requirement R1 Part 1.2.

The SDT chose to include “SCI identified independently supporting…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset’s supporting hardware’s impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be the focus of Requirement R1 Part 1.1.

Rationale for Requirement R1 Part 1.3

The SDT chose to include “SCI identified independently supporting…” language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset’s supporting hardware’s impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be the focus of Requirement R1 Part 1.3.

The addition of “For each change *to the items listed in Part 1.1*” is used to scope the changes to only those listed in Requirement R1 Part 1.1, as a replacement to “deviations from the existing baseline configuration”, of applicable systems.

The addition of CIP Exceptional Circumstances (CEC) to Requirement R1 Part 1.3.1 was made because verification and documentation of cyber security controls prior to emergency change could impede Responsible Entities' efforts to recover from events or conditions that qualify as CEC.

Rationale for Requirement R1 Part 1.4

The addition of "For each change *to the items listed in Part 1.1 or Part 1.2*" is used to scope the changes to only those listed in Requirement R1 Part 1.1 or 1.2, as a replacement to "deviations from the existing baseline configuration", of applicable systems.

The SDT chose to remove the reliance on a "Technical Feasibility Exception" in favor of the updated term "per system capability." The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception (TFE).

Additionally, the SDT chose to add to the phrase "that minimizes adverse effects" with "and differences with the production environment" to eliminate the dependency on baseline configuration. The SDT also enabled CIP-010-5 for the use of Remediation VLANs for testing. This Remediation VLAN is not be considered a part of the production BCS environment and could help facilitate a secure means of testing prior to implementing the change in the production BCS environment.

The addition of CEC to Requirement R1 Part 1.4.1 was made because testing in a test environment and documenting test results may impede Responsible Entities' efforts to recover from events or conditions that qualify as CEC.

Rationale for Requirement R1 Part 1.5

The SDT chose to include "SCI identified independently supporting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset's supporting hardware's impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS and should therefore be the focus of Requirement R1 Part 1.4.

The removal of "deviations from the existing baseline configuration" is a conforming change, with direct references to the specific Requirement R1 Part 1.1, sub-parts 1.1.1, and 1.1.2.

Requirement R2

General Considerations for Requirement R2

The SDT chose to include "SCI identified independently supporting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset's supporting hardware's impact on the individual Cyber Asset itself.

The SDT has added the term "unauthorized" into Requirement R2 Part 2.1 to focus it on the risk of unauthorized changes. Many implementations will perform this task by monitoring all changes and looking for unauthorized changes within that population. However, if a way to filter out authorized changes can be implemented and an entity is able then to monitor just unauthorized changes that should fulfill the requirement.

Requirement R3

General Considerations for Requirement R3

The SDT chose to include "SCI identified independently supporting…" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCAs used in BCS, EACMS, PACS or PCAs. This inclusion also re-emphasizes the criticality of the SCI, due to its inherent capability to affect multiple hosted systems, which could be a significantly broader impact than an individual physical Cyber Asset's supporting hardware's impact on the individual Cyber Asset itself.

Additionally, SCI typically includes supporting management capabilities which allow for the requirement part to be fulfilled on the SCI itself, without reliance on the hosted BCS, EACMS, PACS, or PCAs, and should therefore be a target of this requirement part itself.

Rationale for Requirement R3 Part 3.1

Conforming changes only to Applicable Systems (see General Considerations for Requirement R3 above).

Rationale for Requirement R3 Part 3.2

The SDT chose to remove the reliance on a "Technical Feasibility Exception" in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

In Requirement R3 Part 3.2.1, conforming changes have been made to remove the baseline configuration dependency.

Rationale for Requirement R3 Part 3.3

The timing of when to enforce this requirement part has been an interesting chicken and egg problem. With the inclusion of the language "Prior to becoming a new Applicable System…" the SDT feels it has resolved this issue, and established that before the new system has applicability, i.e. it has an impact to the BES, this requirement part must be fulfilled.

The changes to the Protected Cyber Asset (PCA) definition, and the proposed change mentioned above to the requirement part language, should enable the use of remediation VLANs. The concept of "before connecting to a production environment…" is no longer part if this requirement language.

The requirements have been expanded to assure that virtual machines and their associated infrastructure are properly assessed before they can have an impact to the BES.

Rationale for Requirement R3 Part 3.4

Conforming changes only (see General Considerations for Requirement R3 above).

Requirement R4

General Considerations for Requirement R4

The SDT updated R4 to include associated SCI into the scope of the Transient Cyber Assets (TCA) and Removable Media required plans. The SDT also updated Attachment 1, such that the scope was broadened from a Cyber Asset only solution.

Former Background Section from Reliability Standard CIP-010-4

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.
Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-010-4

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

---

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

---

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019.
https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019.
https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rationale for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to “model” the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Information Protection

Technical Rationale and Justification for Reliability Standard CIP-011-Y

June 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-011-Y

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-011-Y. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-011-Y is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

General Considerations

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-011-Y to align information protection requirements with the virtualization changes.

Requirement R1 and R2

Rationale

The SDT added the option (known as the “all-in” scenario) for entities to group SCI within a BCS it supports; Therefore, to enable CIP-011-Y for virtualization, the SDT added “SCI identified independently supporting an Applicable System above” each of the Parts in Applicable Systems for Requirement R1 – Requirement R2 to account for the alternative option (See the CIP-002 Technical Rationale document for a description of the options for identifying SCI and reasons an entity may choose between the options.)

Requirement R2 Part 2.1

Requirement R2 Part 2.1 is an objective level requirement focused on protecting BES Cyber System Information (BCSI) rather than ‘Cyber Assets’ and ‘storage media’, and modified to include Requirement R2 Part 2.2. This modification creates necessary flexibility, allowing for cryptographic erasure in scenarios where BCSI cannot be mapped to particular disks within virtualized storage, and where BCSI is stored on SCI employing deduplication. This adjustment is also future-looking to better position CIP-011 for the enablement of cloud type scenarios where the disks are owned and/or managed by a third-party as a service to the entity for its BCSI storage, analysis, or use.

Requirement R2 Part 2.2

Requirement R2 Part 2.2 has been deleted because it was consolidated into Requirement R2 Part 2.1.

Former Background Section from Reliability Standard CIP-011-2

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.
The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-011-2

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-011-2 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

> Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.
>
> In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-3

June 2021

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-013-3

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-3. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-013-3 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-013-3 to align supply chain risk management requirements with the virtualization changes.

The SDT added the option (known as the "all-in" scenario) for entities to group SCI within a BCS it supports; Therefore, to enable CIP-013-3 for virtualization, the SDT added "SCI identified independently supporting these BCS or their associated EACMS and PACS" to account for the alternative option (See the CIP-002 Technical Rationale document for a description of the options for identifying SCI and reasons an entity may choose between the options.) Additionally, the SDT simplified the applicability in Requirement R1 Parts 1.1-1.2 by replacing the long list of Applicable Systems with a reference to the list in the parent Requirement R1 through the use of this language, "of systems listed in R1".

Technical Rationale for Reliability Standard CIP-013-2

This section contains a “cut and paste” of the Technical Rationale for CIP-013-2 standard to preserve any historical references.

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team’s (SDT’s) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission’s Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17,

2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).-

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

---

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

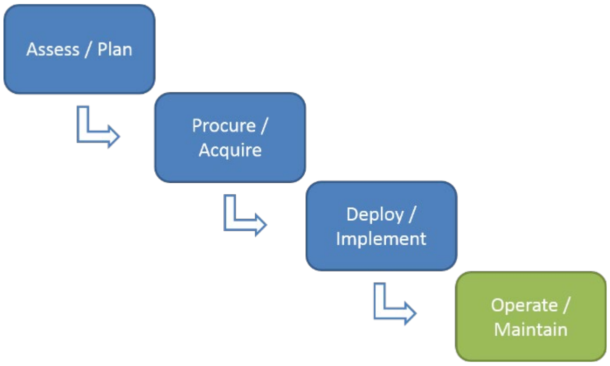
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R3

General Considerations for Requirement R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a “cut and paste” of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).-

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

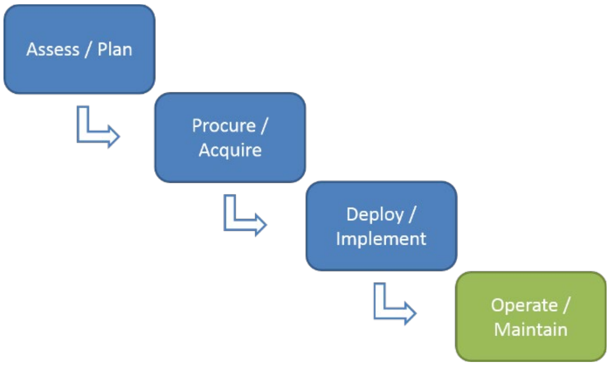
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

UPDATED

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Formal Comment Period Extended, Now Open through September 1, 2021

Now Available

Due to numerous requests received from industry, the 45-day formal comment period for the **CIP Virtualization suite of standards (outlined below)** has been extended and is now open through **8 p.m. Eastern, Wednesday, September 1, 2021**.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-Y - Cyber Security – Security Management Controls
- CIP-004-Y - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-Y - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page**.**

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*

- *Please be mindful of ballot and comment period closing dates. We ask to* ***allow at least 48 hours*** *for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts* ***prior to the last day*** *of a comment/ballot period.*

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **August 23 – September 1, 2021**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization - Draft 2
Comment Period Start Date:	6/30/2021
Comment Period End Date:	9/1/2021
Associated Ballots:	2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 AB 2 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 AB 2 ST

There were 93 sets of responses, including comments from approximately 218 different people from approximately 137 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Are the two options for identification of SCI within CIP-002 clear and is it understood that when SCI is included in the CIP Systems that it is treated like the CIP System, it is a part of for CIP Requirement Applicability?

2. The Applicable Systems column may include "SCI identified independently…" Is this clear or is additional clarification (such as "SCI identified as supporting, but not part of…") needed?

3. The SDT modified the ERC definition to reference "outside the asset containing". This is to allow scoping based on connectivity of the logging systems as required by CIP-007 Requirement R4 as well as the scoping of requirement parts in CIP-004 and CIP-006 based on risk. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

4. The SDT proposes that the modified ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

5. The SDT modified the IRA definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

6. The SDT modified the Management Interface definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

7. As discussed in the CIP Definitions and Exemptions Technical Rationale (TR), the SDT believes that the use of configurations or policy in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

8. The SDT added new and revised several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

9. The SDT revised CIP-002 based on industry comments. Do you agree with the proposed changes to the CIP-002 Reliability Standard? If not, please provide the basis for your disagreement and an alternate proposal.

10. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

11. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

12. The SDT revised CIP-010 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

13. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 (conforming changes) based on industry comments. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

14. Please provide any additional comments for the SAR drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Midcontinent ISO, Inc.	Bobbi Welch	2	MRO,RF,SERC	ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)	Ali Miremadi	CAISO	2	WECC
					Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Bobbi Welch	MISO	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Michael Del Viscio	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC

Eversource Energy	Christopher McKinnon	3		Eversource 1	Christopher McKinnon	Eversource Energy	3	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Portland General Electric Co.	Daniel Mason	6		PGE FCD	Ryan Olson	Portland General Electric Co.	5	WECC
					Nathaniel Clague	Portland General Electric Co.	1	WECC
					Angela Gaines	Portland General Electric Co.	3	WECC
					Daniel Mason	Portland General Electric	6	WECC
Snohomish County PUD No. 1	Holly Chaney	3		SNPD Voting Members	John Martinsen	Public Utility District No. 1 of Snohomish County	4	WECC
					John Liang	Snohomish County PUD No. 1	6	WECC
					Sam Nietfeld	Public Utility District No. 1 of Snohomish County	5	WECC
					Alyssia Rhoads	Public Utility District No. 1 of Snohomish County	1	WECC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC

					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,NA - Not Applicable,RF,SERC,Texas RE,WECC	ACES Standard Collaborations	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Nick Fogleman	Prairie Power, Inc.	1	SERC
					Amber Skillern	East Kentucky Power Cooperative	1	SERC
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	4	MRO
					Fred Meyer	Algonquin Power Co.	1	MRO
					Jamie Monette	Allete - Minnesota Power, Inc.	1	MRO
					Jodi Jensen	Western Area Power Administration - Upper Great Plains East (WAPA)	1,6	MRO
					John Chang	Manitoba Hydro	1,3,6	MRO

					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc.	2	MRO
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1,3,5	MRO
					Joe DePoorter	Madison Gas and Electric	4	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					Bill Shultz	Southern Company Generation	5	MRO
Southwest Power Pool, Inc. (RTO)	Kimberly Van Brimer	2	MRO,WECC	Southwest Power Pool Standards Review Group (SSRG)	Kim Van Brimer	SPP	2	MRO
					Jim Williams	SPP	2	MRO
					Matt Harward	SPP	2	MRO
					Shannon Mickens	SPP	2	MRO
					Alan Wahlstrom	SPP	2	MRO

FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Carey	FirstEnergy - FirstEnergy Solutions	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		CHPD	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company -	5	SERC

						Southern Company Services, Inc. - Gen		
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC

Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
Nurul Abser	NB Power Corporation	1	NPCC
Randy MacDonald	NB Power Corporation	2	NPCC
Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
Vijay Puran	NYSPS	6	NPCC
ALAN ADAMSON	New York State Reliability Council	10	NPCC
Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
Brian Robinson	Utility Services	5	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Jim Grant	NYISO	2	NPCC
John Pearson	ISONE	2	NPCC
Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
Chantal Mazza	Hydro-Quebec	2	NPCC
Michele Tondalo	United Illuminating Co.	1	NPCC
Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC

					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Scott Miller	Scott Miller		SERC	MEAG Power	Roger Brand	MEAG Power	3	SERC
					David Weekley	MEAG Power	1	SERC
					Steven Grego	MEAG Power	5	SERC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay	6	SPP RE	OKGE	Sing Tay	OGE Energy - Oklahoma	6	MRO
					Terri Pyle	OGE Energy - Oklahoma Gas and Electric Co.	1	MRO
					Donald Hargrove	OGE Energy - Oklahoma Gas and Electric Co.	3	MRO
					Patrick Wells	OGE Energy - Oklahoma Gas and Electric Co.	5	MRO
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
		5			Michael Shaw	LCRA	6	Texas RE

Lower Colorado River Authority	Teresa Krabe			LCRA Compliance	Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC

					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. Are the two options for identification of SCI within CIP-002 clear and is it understood that when SCI is included in the CIP Systems that it is treated like the CIP System, it is a part of for CIP Requirement Applicability?

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The proposed definition of CIP System is confusing. Dominion Energy recommends removing CIP System from the proposed defined terms and all references to the CIP System defined term throughout the definitions. Dominion Energy recommends addressing the issues of applicability it appears the CIP System definition was intending to do at the Standard level.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
It is understood that when SCI is included in the CIP Systems it is to be treated like the CIP System. However, the other option for identification of SCI is not clear, as discussed in greater detail in the response to question 2.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
It is understood that when SCI is included in the CIP Systems it is to be treated like the CIP System. However, the other option for identification of SCI is not clear, as discussed in greater detail in the response to question 2.	
Likes 0	

Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Consider modification of SCI to be based on the Cyber Asset definition. SCI's basis on the "programmable electronic devices" terminology makes it unclear as to what type of devices are the intended target of the standard. CIP-002 provides guidance for identification and classification of BCS (grouping of BCAs). Other associated cyber assets are classified based on their connectivity, protection and relationship to the BCAs. Suggest remove SCI identification from CIP-002.	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	No
Document Name	
Comment	
The current definitions and requirement language place BCS, which are groups of Cyber Assets, at the same level as SCI. SCI is likely to be handled as individual devices. This adds complexity both to the CIP-002 R1 compliance process as well as creates complexity for CIP-002 R2.2 approval processes. Duke Energy requests that the SDT add a definition and update requirements to leverage the concept of an SCI Group (SCIG). This would establish parity between the BCA -> BCS relationship with SCI -> SCIG. This also further simplifies applicability in the downstream standards from the current "High Impact BES Cyber Systems (BCS) and their associated: EACMS; PACS; and PCA" with a separate line for "SCI identified independently supporting an Applicable System above" to "High Impact BES Cyber Systems (BCS) and their associated: EACMS; PACS; PCA; and SCIG". Further, the CIP-002 language can now be simplified to the following, which retains closer parity with current language while still addressing the SDT's intentions: "Identify each of the high impact BES Cyber Systems, if any, and associated Shared Cyber Infrastructure Groups, if any, according to Attachment 1, Section 1 at each asset".	
Likes 0	
Dislikes 0	
Response	

Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
We believe the options are mostly clear and acceptable with the exception of the phrase “independent SCI supporting” either high or medium impact. It is unclear and confusing how an SCI can be both independent and supporting simultaneously. The proposed revised definition of BES Cyber System already would make it clear that SCI is to be included in CIP scope if applicable. We recommend removing the second bullet point entirely from both R1.1 and R1.2.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
The identification of SCI is not clear within CIP-002, nor is it understood that SCI should be high-water marked to the highest impact applicable system that is sharing its infrastructure. The only thing that makes this clear is the definition of CIP System, which term is not used within CIP-002.	
Likes 0	
Dislikes 0	
Response	

William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
The identification of SCI included in a CIP System is clear but the identification of Management Systems included in SCI is unclear. For the all-in scenario, with Provider1 as an example, the Provider management Cyber Asset would typically be outside the ESP currently. With the new all-in, that CA would be a Management Interface, and would then be included as part of the SCI per the SCI 'including Management Interfaces' definition, which would then pull the CA into the BCS, making it a BCA, so it can no longer be outside of the ESP.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
It is confusing to understand the definition of Shared Cyber Infrastrure (SCI) and therefore the overall requirement is unclear. While significant education to industry would improve this, it is extremely dependent on interpretation by stakeholders and auditors.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
The CIP-002 should maintain a section on BROS that establish the relationship with the BCS	
Likes 0	
Dislikes 0	
Response	

Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	No
Document Name	
Comment	
We believe the options are mostly clear and acceptable with the exception of the phrase “independent SCI supporting” either high or medium impact. It is unclear and confusing how an SCI can be both independent and supporting simultaneously. The proposed revised definition of BES Cyber System already would make it clear that SCI is to be included in CIP scope if applicable. We recommend removing the second bullet point entirely from both R1.1 and R1.2. On a related note, we are concerned about revising the existing CIP standards to address virtual technologies and believe a better approach may be to address the majority of impacts and new requirements in a new standard. Please see our comment on this in response to question #14.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The term 'SCI' is still unclear and ambiguous.The term 'SCI' is still unclear and ambiguous.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA supports the “All-In” option which identifies the SCI is to receive the impact rating based on the BCS that it hosts. It is not clear how the identified independently option is to be evaluated.	
Likes 0	

Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	No
Document Name	
Comment	
It is not clear what is meant by independent SCI supporting any part of the high impact BCS.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE does not agree that the two options for identification of SCI are clear. The distinction between SCI included in a BES Cyber System (BCS) and SCI operating independently adds an unnecessary level of complexity to the standards. Texas RE recommends there be only one option, which is to categorize SCI as meeting the definitions of the VCAs they are hosting and subsequently include the SCI within BCS, Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) and Protected Cyber Assets (PCAs), as applicable. Additionally, Texas RE recommends that registered entities be required to identify all BCS, as well as their associated EACMS, PACS, and PCAs, as applicable. System (PM5) and system component (CM-8) inventory are both controls from NIST 800-53 Rev. 5. Texas RE is concerned CIP-002-7 would be less effective if registered entities are not required to implement the full suite of the system and component inventory protections in a manner consistent with these requirements.	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We support NPCC TFIST's comments as found below: Request clarification when a SCI supports both high impact BES and medium impact BES. Is that SCI high watermarked to the high impact? Request clarification of "it is a part of for CIP Requirement Applicability?" Is there a missing word? Should the language be "it is a part of it for CIP Requirement Applicability?" Request clarification of the or in 1.3. Is the entity identifying low impact BCS or supporting SCI or both? Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
The standard is clear about the two options. However, the Technical Rationale it is not clearly understood how the Standards Drafting Team anticipates treatment of systems.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
In support of NPCC RSC comments.	

Request clarification when a SCI supports both high impact BES and medium impact BES. Is that SCI high watermarked to the high impact?

Request clarification of “it is a part of for CIP Requirement Applicability?” Is there a missing word? Should the language be “it is a part of it for CIP Requirement Applicability?”

Request clarification of the or in 1.3. Is the entity identifying low impact BCS or supporting SCI or both?

Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?

We don’t understand how to categorize a Shared Cyber Infrastructure. The SDT seems to make a distinction between two types of SCI, one type is supporting, and the other type is independent supporting. Our hypothesis is that a “supporting SCI” is for BCS (BCA/PCA) and that an “independent supporting SCI” is for associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS)).

In both cases, the SCI is the categorization labels, like BCA, PCA, EACMS, PACS, TCA.

Yet in the Applicable Systems column in the other CIPs, the SDT seem to make a distinction between the SCI, for example

CIP-005 R1.5 1.5 … PACS hosted on SCI … SCI identified independently…

CIP-007 R1.1 SCI identified independently supporting.

Clarification is needed.

Are the two options for identification SCI required? Is there a difference in the controls that we want to apply?

We suggest simplifying the language or add more precision. Example:

Per Attachment 1, Section 1, identify each high impact BES Cyber System as either of the following, if any, at each asset; High Impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), Protected Cyber Assets (PCAs) or SCI.

Furthermore, in the definition of SCI the PCA is not listed. Is this intentional? Wouldn’t be possible to have a PCA supported by an SCI? We suggest that the SDT review the SCI / VCA/ PCA definitions, adjust the applicability and the requirements.

Reference SCI: One or more programmable electronic devices, including the software and Management Interfaces, that share: • CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, or PACS; or

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

While AEP agrees with the inclusion of this CIP-002 mechanism (the term CIP Systems) for including the associated applicable systems (EACMS, PACS, and PCAs) as a means to have a singular requirement for the identification of EACMS, PACS and PCAs, the current language appears to limit the identification of only those virtual systems (and underlying infrastructure) related to EACMS, PACS and PCAs. We believe this leaves a gap for the identification of those physical systems performing the same function(s). We recommend SDT to add clarifying language to allow for the identification of both physical and virtual systems as EACMS, PACS and PCAs under CIP-002.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

IESO supports the comments submitted to all the questions by both NPCC and ISO/RTO Council

Request clarification when a SCI supports both high impact BES and medium impact BES. Is that SCI high watermarked to the high impact?

Request clarification of “it is a part of for CIP Requirement Applicability?” Is there a missing word? Should the language be “it is a part of it for CIP Requirement Applicability?”

Request clarification of the or in 1.3. Is the entity identifying low impact BCS or supporting SCI or both?

Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?

We don’t understand how to categorize a Shared Cyber Infrastructure. The SDT seems to make a distinction between two types of SCI, one type is supporting, and the other type is independent supporting. Our hypothesis is that a “supporting SCI” is for BCS (BCA/PCA) and that an “independent supporting SCI” is for associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS)).

In both cases, the SCI is the categorization labels, like BCA, PCA, EACMS, PACS, TCA.

Yet in the Applicable Systems column in the other CIPs, the SDT seem to make a distinction between the SCI, for example

CIP-005 R1.5 1.5 … PACS hosted on SCI … SCI identified independently…

CIP-007 R1.1 SCI identified independently supporting.

Clarification is needed.

Are the two options for identification SCI required? Is there a difference in the controls that we want to apply?

We suggest simplifying the language or add more precision. Example:

Per Attachment 1, Section 1, identify each high impact BES Cyber System as either of the following, if any, at each asset; High Impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), Protected Cyber Assets (PCAs) or SCI.

Furthermore, in the definition of SCI the PCA is not listed. Is this intentional? Wouldn't be possible to have a PCA supported by an SCI? We suggest that the SDT review the SCI / VCA/ PCA definitions, adjust the applicability and the requirements.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	Independently Identified SCI.jpg

Comment

The phrases "supporting SCI" and "independent SCI supporting" are not clear and should be removed from CIP-002. Resulting from SCI definition, SCI should be either a CIP cyber asset or no-CIP cyber asset, therefore SCI shouldn't appear in CIP-002 and Applicable Systems of CIP-003 to CIP-013. SCI should be used for identifying additional BCAs, EACMS, PACS or PCAs that could be missed in the virtualization environment.

For the proposed All-in-Scenario, SCI should be identified as a BCA, EACMS, PACS or PCA rather than a new classification of CIP cyber asset. For example, if a SCI can initialize, deploy and configure a BCA, it should be categorized as a BCA since it can remove a virtual BCA thus having an impact to the BES within 15 minutes. Similarly, if a SCI can initialize, deploy and configure an EACMS, it should be categorized as an EACMS since it can remove the virtual EACMS thus having electronic control function.

For independently Identified SCI as SDT proposed below, for the right side SCI, if the right SCI containing Management Interface can initialize, deploy and configure a CIP Cyber Asset, it should be categorized as a CIP cyber asset (See our comments above). If the right-side SCI hosts VCA that is a CIP cyber asset regardless of the impact rating, the right side SCI should be identified as the same impact CIP cyber asset it hosts. The right side SCI is out of CIP scope only: (1) if all VCAs it hosts are non-CIP cyber assets, this SCI would be out of CIP scope thus no need to be identified; (2) If it is used only to configure high impact network policy, it would be out of CIP scope since out of band management for CIP cyber assets is not required by the current CIP requirements scope and the SAR

Based on our comments above, the "SCI" and "independently Identified SCI" are not needed to be identified in CIP-002 since the SCI or independently Identified SCI either is a CIP cyber asset or out of CIP scope.

SEE ATTACHED DOCUMENT FOR PHOTO.

Resulting from our comments above, we recommend revising definitions of BCA, EACMS, PACS and PCA to include SCI so SCI would not be identified as another independently applicable CIP cyber asset. Our proposed changes align with FERC and NERC's security objectives and the SDT's goal to address cyber security risks to the reliability of the BES from virtualization technologies, while having less impact on the entities existing CIP programs, processes and documentation. Entities can use their existing CIP cyber asset identification processes to identify BCAs, EACMS, PACS and PCAs based on SCI and Management Interface language to address virtualization. If the responsible entities don't have virtualization, they wouldn't need to identify any additional CIP cyber assets at all.

Recommendations:

1. Restore the CIP-002 R1 and its Parts resulting from our proposed definitions changes below.

2. We propose the following changes to the new or existing definitions:

SCI:

SDT Proposed SCI definition

One or more programmable electronic devices, including the software and Management Interfaces, that share:

- CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, or PACS; or
- storage resources with any part of a BES Cyber System or their associated EACMS or PACS.

Each SCI is either:

- included in one or more BES Cyber Systems, EACMS, or PACS; or
- identified independently.

SCI does not include the supported VCA or CA with which it shares its resources.

NSRF Proposed Changes to the Definition

One or more programmable electronic devices, including the software and Management Interfaces in those devices, that share:

- CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, PACS or PCA; or
- storage resources with any part of a BES Cyber System or their associated EACMS, PACS or PCA.

This includes devices that contain Management Interfaces for virtualization management.

SCI does not include the supported VCA or CA with which it shares its resources.

Rationale: In the SDT proposed SCI definition, the device containing Management Interface is left out and is not identified as a CIP cyber part of SCI even though the management interface is in scope. For example, vCenter containing Management Interface, but it is not identified as a CIP cyber asset and is not protected. Also, PCA is missing from the SCI definition. In our proposed changes, it is not necessary to identify SCI independently since SCI would be identified as one of CIP Cyber Assets.

Management Interface:

SDT Proposed SCI definition

A user interface, logical interface, or dedicated physical port that is used to:

- Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or
- Provide lights-out management capabilities; or
- Configure an Electronic Security Perimeter;

excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Our Proposed Changes to the Definition

A user interface, logical interface, or dedicated physical port that is used to:

- Initialize, deploy, and configure BCA, EACMS, PACS, or PCA; or
- Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or
- Configure EAP of an Electronic Security Perimeter; or
- Configure EACMS that controls all communications to and from the BCS unless ESP model is used.

excluding physical user interfaces (e.g., power switch, touch panel, etc.). (See our rationale in Q6).

Rationale: In our view, the definition should focus on “in scope” CIP management interfaces. The term “Provide lights-out management capabilities” is not clear and should be removed since this criterion itself cannot make a management interface fall within CIP scope.

Also, the Management Interface on the SCI is absent. We have added a bullet in our proposed definition to address it.

Furthermore, we suggest edits to include:

a) changing configure an ESP to configure an EAP

b) adding configure EACMS to address the zero-trust mode based on our comments in Q4.

BCA:

SDT Proposed SCI definition

A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded , or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Our Proposed Changes to the Definition

A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. This includes SCI that is used for initializing, deploying and configuring BCAs or storing information for the real-time operation of BCAs.

Rationale: In our view, if a SCI meets BCA criteria, it must be identified as a BCA.

EACMS:

SDT Proposed SCI definition

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Intermediate Systems and SCI grouped, by the Responsible Entity, in the EACMS it supports.

Our Proposed Changes to the Definition

Cyber Assets or Virtual Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems and SCI that is used for initializing, deploying and configuring EACMS or storing information for the real-time operation of EACMS.

Rationale: A SCI supporting EACMS doesn't make it to be part of EACMS. For instance, if a SCI only stores historical information for EACMS, it could be a BCSI repository rather than part of EACMS. In our view, only a SCI that can initialize, deploy and configure EACMS should be identified as EACMS.

PACS:

SDT Proposed SCI definition

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) (including SCI grouped, by the Responsible Entity, in the Physical Access Control Systems it supports) that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Our Proposed Changes to the Definition

Cyber Assets or Virtual Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. This includes SCI that is used for initializing, deploying and configuring PACS or storing information for the real-time operation of PACS.

Rationale: A SCI supporting PACS doesn't make it to be part of PACS. For instance, if a SCI only stores historical information for PACS, it could be a BCSI repository rather than part of PACS. In our view, only a SCI that can initialize, deploy and configure PACS should be identified as PACS.

PCA:

SDT Proposed SCI definition

One or more Cyber Assets or Virtual Cyber Assets that:

- Are within an Electronic Security Perimeter but are not part of the highest impact BES Cyber System within the same Electronic Security Perimeter; or
- Share CPU or memory with any part of a BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to the Electronic Security Perimeter.

Our Proposed Changes to the Definition

One or more Cyber Assets or Virtual Cyber Assets that:

- Are within an Electronic Security Perimeter but are not part of the highest impact BES Cyber System within the same Electronic Security Perimeter; or
- Share CPU or memory with any part of a BES Cyber System, EACMS, PACS or PCA; or

This includes SCI that is used for initializing, deploying and configuring PCA or storing information for the real-time operation of PCA.

Rationale: In the SDT proposed PCA definition, if the bullet 2 is for identifying PCA that shares resources with BCS, the ESP should be irrelevant. Also, it is not clear what the remediation actions are and why the one-time remediation makes it out of scope, noting that the compliance is an ongoing basis and the remediation shouldn't exclude a VCA from CIP scope. Furthermore, if SDT intends to protect non-CIP cyber assets that share the CPU or memory with CIP cyber assets, EACMS, PACS and PCA sharing resources with non-CIP cyber assets should also be considered rather than only BCS.

CA: Restore the CA definition.

Rationale: Given that SCI is defined as a programmable device, it meets the CA definition and should be treated as one type of CAs rather than excluding it from CA definition.

VCA: A logical instance of an operating system or firmware including software, data and virtual hardware on the logical instance hosted on a physical Cyber Asset.

BCS: Restore BCS definition.

Rationale: BCS should only include BCAs not other CIP cyber assets. Given that SCI could be an EACM, PACS or PCR, it shouldn't be included in BCS definition.

CIP System: This definition is not needed based on our proposed changes above.

Rationale: CIP System won't work for the CIP requirements since not each requirement applies to all CIP cyber assets that are included in the CIP System and the requirement has to specified which CIP cyber asset would apply.

ERC: Restore ERC definition since it is still effective (see our rationale in Q3).

EAP: Restore the definition

Rationale: Given that the current EAP is still clear and doesn't exclude policy-based rules, there is no need to modify EAP definition.

ESP: Restore ESP definition since it is still effective for the perimeter-based network protection (see the rationale in Q4).

IRA:

SDT Proposed SCI definition

User-initiated real-time access by a person from outside of the Responsible Entity's Electronic Security Perimeters (ESP) using a routable protocol:

- to a Cyber System within an ESP;
- through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;
- To Management Interfaces of Shared Cyber Infrastructure; or
- To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforces an ESP.

Our Proposed Changes to the Definition

User-initiated interactive access by a person employing a remote access client or other remote access technology using a routable protocol. (This includes cases where a routable protocol is converted to a non-routable protocol)

Remote access originates from a Cyber Asset or Virtual Cyber Asset that is:

a. not an Intermediate System

b. is not located within any of the Responsible Entity's Electronic Security Perimeter(s) or,

c. at a defined Electronic Access Point (EAP).

Interactive remote access does not include system-to-system process communications. (See our rationale in Q5).

Rationale: IRA definition should only define what remote access constitutes an IRA and shouldn't include the accessed end devices. The IRA accessed cyber assets should be addressed in the requirements rather than in the IRA definition. We propose to add additional language to clarify the routable protocol converting to non-routable still falls within IRA definition since the current IRA definition is not clear on this. The current IRA definition states the user-initiated access using a routable protocol and doesn't say all communication sessions need to be routable.

Intermediate System: Restore the IS definition since the current definition is clear and no need to redefine it.

Rationale: The proposed IS definition starts from "EACMS", which is not correct logically. A Cyber Asset should meet the IS definition and then becomes an EACMS. Otherwise an IS can be missed if it is not an EACMS originally.

BCSI: Restore the definition based on our proposed definition changes above.

Cyber Security Incident: Restore the definition based on our proposed definition changes above.

PSP: Restore the definition based on our proposed definition changes above.

Removable Medium: Restore the definition based on our proposed definition changes above.

Reportable Cyber Security Incident: Restore the definition based on our proposed definition changes above.

TCA: Restore the definition based on our proposed definition changes above.

We believe the options are mostly clear and acceptable with the exception of the phrase "independent SCI supporting" either high or medium impact. It is unclear and confusing how an SCI can be both independent and supporting simultaneously. The proposed revised definition of BES Cyber System already would make it clear that SCI is to be included in CIP scope if applicable. We recommend removing the second bullet point entirely from both R1.1 and R1.2.

Likes 0	
Dislikes 0	

Response

Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5

Answer	No
Document Name	

Comment

Recommend spelling out "Shared Cyber Infrastructure" and its acronym within the standard text.

Recommend including the definition within the text, or make a statement in the text directing to the definition in the definition list.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

The options for SCI association within CIP-002 may be clear, but the handling of SCI involving EACMS cases is not clear from CIP-002 since that standard is limited to assessment of HIGH, MEDIUM and LOW impact BCS cases.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

In support of IRC SRC/SWG.

Request clarification when a SCI supports both high impact BES and medium impact BES. Is that SCI high watermarked to the high impact?

Request clarification of “it is a part of for CIP Requirement Applicability?” Is there a missing word? Should the language be “it is a part of it for CIP Requirement Applicability?”

Request clarification of the OR in 1.3. Is the entity identifying low impact BCS OR supporting SCI OR both?

Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Independent SCI supporting and supporting SCI are not clear. They should be removed from CIP-002.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The only exception of the phrase “independent SCI supporting” either high or medium Impact. The statement is unclear and confusing how an SCI can be both indendent and supporting sitmultaneously. The proposed revised definition of the BES Cyber System already would make it clear that SCI is to be included in CIP scope if applicable, It is recommended removing the second bullet entirely from both R1.1 and R1.2.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	

We thank the SDT for it’s work but believe the changes to definitions will create greatly impact existing entity’s policies, procedures and documentation and increase administrative overhead when some basic changes can be drafted which will a) retain and address the issue of virtualization, b) allow entity’s the flexibility to identify risks and implement appropriate security controls, and c) clarify language for regulators and industry alike. The current drafts create much administrative overhead because it requires entity’s using virtual platforms to parse out subcomponents and assign risk to establish compliance for such components. As entity’s move to cloud environments this will not be possible and therefore it is more practical to allow entity’s to identify their systems, assess risk and categorize them based on hardware profiles. SCI does little to clarify and define. In general, WAPA recommends a focus on individual hardware components and software enforcment policies (AAA). For example, an entity could consider an ESXi platform a single BCS (or BCA) which contains VCAs. Just a perspective.

The phrases “supporting SCI” and “independent SCI supporting” are not clear and should be removed from CIP-002. Recommend that SCI should be either categorized as a CIP Cyber Asset or not a CIP Cyber Asset (Hardware based decision). SCI shouldn’t appear in CIP-002 and Applicable Systems of CIP-003 to CIP-013. SCI should be evaluated using the criteria of a BCAs, EACMS, PACS or PCAs which can be missed in the virtualization environment.

For the proposed All-in-Scenario, SCI should be identified based on hardware such as BCA, EACMS, PACS or PCA rather than a new classification of CIP cyber asset. Creating separate definitions for SCI is tantamount to identifying hard drives and PCI cards as separate BCA and this will require entity’s a great deal of administrative overhead.

Secondly, SCI that can initialize, deploy and configure a BCA should be categorized as a BCA since it has a high risk profile - can remove a virtual BCA and impact to the BES within 15 minutes. Similarly, if a SCI can initialize, deploy and configure an EACMS and should be categorized as an EACMS since it can remove the virtual EACMS and it’s functions.

For independently Identified SCI proposed in the right box diagram below, SCI with an active Management Interface can initialize, deploy and configure a CIP Cyber Asset. This further supports the case for categorization based on hardware and not sub-components.

If the right-side SCI hosts VCA such as a CIP cyber asset regardless of the impact rating, the right side SCI should be identified as the same impact CIP cyber asset it hosts. It has the capability to impact the BES in 15 minutes. The right side SCI is out of CIP scope only: (1) if all VCAs it hosts are non-CIP cyber assets, this SCI would be out of CIP scope thus no need to be identified; (2) If it is used only to configure high impact network policy, it would be out of CIP scope since out of band management for CIP cyber assets is not required by the current CIP requirements scope and the SAR

Based on our comments above, the “SCI” and “independently Identified SCI” are not needed to be identified in CIP-002 since the SCI or independently Identified SCI either is a CIP BES Cyber Asset or not in scope.

We recommend revising definitions of BCA, EACMS, PACS and PCA to include SCI. Our proposed changes align with FERC and NERC’s security objectives and the SDT’s goal to address cyber security risks to the reliability of the BES from virtualization technologies, while having less impact on the entities existing CIP programs, processes and documentation. Entities can use their existing CIP cyber asset identification processes to identify BCAs, EACMS, PACS and PCAs based on SCI and Management Interface language to address virtualization. If the responsible entities don’t have virtualization, they wouldn’t need to identify any additional CIP cyber assets at all.

Recommendations:

1. Restore the CIP-002 R1 and its Parts resulting from our proposed definitions changes below.
2. We propose the following changes to the new or existing definitions:

SCI: One or more programmable electronic devices, including the software and Management Interfaces in those devices, that share:

- CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, PACS or PCA; or
- storage resources with any part of a BES Cyber System or their associated EACMS, PACS or PCA.

- Includes devices that contain Management Interfaces for virtualization management.
- SCI does not include the supported VCA or CA with which it shares its resources.

Basis for this Recommendation: PCA is missing from the SCI definition. In our proposed changes, it is not necessary to identify SCI independently since SCI would be identified as a CIP Cyber Asset(s).

Management Interface: A user interface, logical interface, or dedicated physical port that is used to:

- Initialize, deploy, and configure BCA, EACMS, PACS, or PCA; or
- Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or
- Configure EAP of an Electronic Security Perimeter; or
- Configure EACMS that controls all communications to and from the BCS unless ESP model is used.
- Excludes physical user interfaces (e.g., power switch, touch panel, etc.). (Refer to Q6).

Basis for this Recommendation: the definition should focus on “in scope” CIP management interfaces. The term “Provide lights-out management capabilities” is not clear and should be removed since this criterion itself cannot make a management interface fall within CIP scope.

- Also, the Management Interface on the SCI is absent. We have added a bullet in our proposed definition to address it.
- Furthermore, we suggest edits to include:
- a) changing configure an ESP to configure an EAP
- b) adding configure EACMS to address the zero-trust mode based on our comments in Q4

CA: Restore the CA definition.

Basis of this Recommendation: If SCI is defined as a programmable device, it meets the definition of a CA and should be treated as one type of CA’s rather than excluding it from CA definition.

VCA: A logical instance of an operating system or firmware including software, data and virtual hardware on the logical instance hosted on a physical Cyber Asset.

BCS: Restore BCS definition.

Basis of this Recommendation: BCS should only include BCAs not other CIP cyber assets. Given that SCI could be an EACM, PACS or PCR, it shouldn’t be included in BCS definition.

CIP System: This definition is not needed based on our proposed changes above.

Basis of this Recommendation: CIP System won't work for the CIP requirements since not each requirement applies to all CIP cyber assets that are included in the CIP System and the requirement has to specified which CIP cyber asset would apply.

ERC: Restore ERC definition since it is still effective (see our rationale in Q3).

EAP: Restore the definition

Rationale: Given that the current EAP is still clear and doesn't exclude policy-based rules, there is no need to modify EAP definition.

ESP: Restore ESP definition since it is still effective for the perimeter-based network protection (see the rationale in Q4).

IRA: User-initiated interactive access by a person employing a remote access client or other remote access technology using a routable protocol. (This includes cases where a routable protocol is converted to a non-routable protocol)

Remote access originates from a Cyber Asset or Virtual Cyber Asset that is:

3. not an Intermediate System
4. is not located within any of the Responsible Entity's Electronic Security Perimeter(s) or,
5. at a defined Electronic Access Point (EAP).

- Interactive remote access does not include system-to-system process communications. (See our rationale in Q5).

Basis for this Recommendation: IRA definition should only define what remote access constitutes as IRA and shouldn't include the accessed end devices. IRA accessed Cyber Assets should be addressed in the requirements rather than in the IRA definition. Recommend additional language to clarify the routable protocol converting to non-routable that falls within IRA definition - since the current IRA definition is not clear on this anyway. The current IRA definition states the user-initiated access using a routable protocol and doesn't refer to communication sessions needing to be routable.

Intermediate System: Restore the IS definition since the current definition is clear and no need to redefine it.

Basis for this Recommendation: The proposed IS definition starts from "EACMS", which is not correct logically. A Cyber Asset should meet the IS definition and then becomes an EACMS. Otherwise an IS can be missed if it is not an EACMS originally.

BCSI: Restore the definition based on our proposed definition changes above.

Cyber Security Incident: Restore the definition based on our proposed definition changes above.

PSP: Restore the definition based on our proposed definition changes above.

Removable Medium: Restore the definition based on our proposed definition changes above.

Reportable Cyber Security Incident: Restore the definition based on our proposed definition changes above.

TCA: Restore the definition based on our proposed definition changes above.

Likes 0	
Dislikes 0	

Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
Please clarify if the SCI “form” as an Cyber System that includes the Management Interface will not require a separate Cyber Asset in the BCS List for the Management Interface provided the SCI Management Interface is the document IP address in CIP-007 R1.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	
Eversource recommends using "Independently identified". The term seems inconsistent in regards to how its used in all the CIP Standards.	
Likes 0	
Dislikes 0	
Response	

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT supports the IRC SRC comments and offers these additional comments:

- R1.1, bullet 1: Under the current version of CIP-002, there is no specific requirement to identify specific types of Cyber Assets applicable to the remaining CIP standards; it is implied at best. Going beyond the BCS identification into identifying specific Cyber Asset types, like Shared Cyber Infrastructure, is a change in to the fundamentals of CIP-002 and takes us back to CIP v1-v4 and the very granular level of Cyber Asset identification. The SDT should determine if all Cyber Asset types should be identified in CIP-002 or not. Each Cyber Asset type under the CIP standards is important in its role, including the SCI. If the SDT does not think that all Cyber Asset types should be addressed, SCI should be removed from this standard.
- R1.1, bullet 2: Please clarify the use of “independent.” It is unclear what this means. Independent of what?
- ERCOT recommends that no changes be made to requirement R1 in CIP-002.

Likes 0	
Dislikes 0	
Response	

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	

While the expectation is clear with regard to what needs to be protected and why, what is not clear is what is required to achieve compliance with CIP-002 R1.1 requirements.

The requirement requires the identification of BCS as either “including any supporting SCI as part of the BCS” or with “independent SCI supporting any part of the high impact BCS or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).” This does not allow for the identification of BCS independent of having SCI, and therefore doesn’t account for non-virtualized environments.

The requirements and measures of CIP-002 do not sufficiently detail what is required to demonstrate compliance. The requirements are to create a list that identifies “each [BCS] as either” including supporting SCI or having independent SCI. However, the independent SCI details an association to EACMS, PACS, PCA. The requirement expects an identification of “BES Cyber Systems” but the sub-bullets imply an expectation to identify SCI and corresponding asset/system classifications. The measures and technical rationale provide no additional clarity other than creating lists. Is the expectation to simply provide identification that the identified BCS either include SCI or are supported by SCI (e.g. Yes/No or Checkbox), or is the expectation to explicitly identify and categorize SCI that meet this criteria (e.g. “1.) ABC High Impact BCS; 2.) CDE High Impact EACMS SCI”). If the expectation is to classify SCI, what should be the approach for classifying SCI that supports multiple classifications (e.g. EACMS and PACS)?

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the IRC SRC.

Likes 0	
Dislikes 0	

Response

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification when a SCI supports both high impact BES and medium impact BES. Is that SCI high watermarked to the high impact?

Request clarification of “it is a part of for CIP Requirement Applicability?” Is there a missing word? Should the language be “it is a part of it for CIP Requirement Applicability?”

Request clarification of the or in 1.3. Is the entity identifying low impact BCS or supporting SCI or both?

Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?

We don’t understand how to categorize a Shared Cyber Infrastructure. The SDT seems to make a distinction between two types of SCI, one type is supporting, and the other type is independent supporting. Our hypothesis is that a “supporting SCI” is for BCS (BCA/PCA) and that an “independent supporting SCI” is for associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS)).

In both cases, the SCI is the categorization labels, like BCA, PCA, EACMS, PACS, TCA.

Yet in the Applicable Systems column in the other CIPs, the SDT seem to make a distinction between the SCI, for example

CIP-005 R1.5 1.5 … PACS hosted on SCI … SCI identified independently…

CIP-007 R1.1 SCI identified independently supporting.

Clarification is needed.

Are the two options for identification SCI required? Is there a difference in the controls that we want to apply?

We suggest simplifying the language or add more precision. Example:

Per Attachment 1, Section 1, identify each high impact BES Cyber System as either of the following, if any, at each asset; High Impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), Protected Cyber Assets (PCAs) or SCI.

Furthermore, in the definition of SCI the PCA is not listed. Is this intentional? Wouldn't be possible to have a PCA supported by an SCI? We suggest that the SDT review the SCI / VCA/ PCA definitions, adjust the applicability and the requirements.

Reference SCI: One or more programmable electronic devices, including the software and Management Interfaces, that share: • CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, or PACS; or

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

The ISO/RTO Council (IRC) Standards Review Committee (SRC) requests clarification of how SCI is to be treated when it supports both high impact BES and medium impact BES; i.e. is the SCI to be watermarked to the highest impact?

Request clarification of "it is a part of for CIP Requirement Applicability?" Is there a missing word? Should the language be "it is a part of it for CIP Requirement Applicability?"

Request clarification of the OR in 1.3. Is the entity identifying low impact BCS OR supporting SCI OR both?

Request clarification of the 1.3 parenthetical. Is the entity required to provide an asset list for either low impact BCS or supporting SCI?

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	Yes
Document Name	

Comment

Chelan approves of this language.

Likes 0	

Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
The shared SCI and TCA definitions are clear and are understood by technical staff; however, the scope included in these definitions may be dfficult to communicate to management staff as written.	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that the two options for identification of SCI within CIP-002 are clear.	
Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
ACES agrees when SCI is included in the CIP Systems it falls into scope of CIP requirements where SCI is an Applicable System. The issue is not with CIP-002's usage of SCI or its definition, but the definition of CIP System as it lacks the inclusion of VCAs which could lead to confusion. AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) agrees that the two options in CIP-002 R1 are clear, due to the explanation in the Technical Rationale, and understands that SCI is an applicable system when it supports an applicable system either as part of the system or as independent SCI.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Southern Indiana Gas and Electric Company (SIGE) agrees that the two options in CIP-002 R1 are clear, due to the explanation in the Technical Rationale, and understands that SCI is an applicable system when it supports an applicable system either as part of the system or as independent SCI.	

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	Yes
Document Name	

Comment

SDG&E supports EEI Comments

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	Yes
Document Name	

Comment

OKGE supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	Yes
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	Yes
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	

Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Yes. The two options for SCI identification are clear within the CIP-002 standard revisions. However, the SDT should provide implementation guidance including examples of how to document the SCI, whether included within the CIP System or independently. Additionally, it would be helpful if the SDT was able to provide Implementation Guidance that included a logic diagram depicting how the device classifications and embedded definitions like Management Interface and CIP System can be applied. In addition, the SDT has been clear that this project focuses on on-premise virtualization, however, many virtualization concepts, like SCI, could be interpreted as being related to use of cloud computing technologies. AWS suggests explicitly stating that the Standards do not apply to cloud within the Applicability section of CIP-002. If these updated Standards do not apply to cloud, it should be obvious to the reader.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees that the two options are clear and it is understood that when a high/medium impact BCS that includes any supporting SCI is identified as a complete BCS (‘all-in’), the SCI is included in CIP requirement applicability wherever a BCS is identified in applicability.	
Likes 0	
Dislikes 0	

Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the two options in CIP-002 R1 are clear based on the explanation contained in the technical rationale, and supports the changes made regarding the identification of SCI within CIP-002.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	2016-02_Virtualization_Unofficial_Comment_Form_(FINAL).docx
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. The Applicable Systems column may include “SCI identified independently…” Is this clear or is additional clarification (such as “SCI identified as supporting, but not part of…”) needed?

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

The existing language, “SCI identified independently supporting an Applicable System” is open to misinterpretation. The IRC SRC recommends the language be clarified by adding a comma to distinguish between “identified independently” and “supporting” as follows: “SCI identified independently, supporting an Applicable System”

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

This language can be misinterpreted. Recommend clarification. Current language is “SCI identified independently supporting an Applicable System.” Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

The context of the question isn't clear is this question a general question or it's pertaining to CIP-002.

Also, the question offers two choices; "Is this clear" or "is additional clarification needed" yet the choices are Yes/No.

So, our answer; is No, it's not clear and yes additional clarification is needed.

Our hypothesis is that it must be a general question. We are not sure of the value of identifying the SCI ("supporting SCI" vs an "independent supporting SCI"), the SCI should be controlled and own requirements.

If the SDT maintains its distinction, they should enforce two types of categorizations and the requirements should be defined with those two types of categorizations in mind.

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Additional guidance is needed for “SCI identified independently.” Also, the phrase “independent SCI supporting…” is not clear. Is this specifically to the VM environment used to create the virtual BCS?	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	

Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	
Additional clarification such as mentioned in Question 1 comment would be a benefit. Also, additional clarity regarding how to group or identify the SCI objects would be beneficial. By chassis, by blade, by host, by logical grouping of functions, etc.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	

Comment

The process for the independent identification of SCI is not clear and needs additional clarification. EEI notes that within the VSLs for CIP-002, "independently identified SCI" is mentioned 27 times, yet no explanation is provided as to what it means or how this is to be accomplished.

It is also not clear what is meant by the term "independent SCI". This term is prominently used in Requirement R1, subpart 1.1 and 1.2 (bullet 2) but not explained. EEI asks that the SDT either define the term or use another term that is more widely understood.

Note: While EEI has identified our concern related to the use of SCI identified independently in CIP-002, this phrase is used throughout the CIP standards. For this reason, the SDT should provide more clarity to this term.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT supports the IRC SRC comments and offers these additional comments:

- Clarify "identified independently supporting". It is unclear what this means. Independent of what?
- Listing the SCI in the applicable systems columns contradicts what was done in the definition of BES Cyber System. The proposed definition of BES Cyber System already includes SCI but does not have the same qualifiers as in the applicable systems column.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern agrees that "SCI identified independently" is clear and no additional clarification of that particular phrase is needed. However, Southern is concerned with the lack of clarity around SCI that does not host a BES Cyber System and is not within an ESP. Specifically, the inclusion of EACMS and PACS within the definition of SCI (and SCI within the EACMS and PACS definitions). As an example, an entity may have a VCA that is involved in processing access control logs. If this is an example of the "M" in EACMS (see discussion of this on Q14), and any part of the process executes as a VCA, then is the entire SCI now in scope? If so, what about backup systems that copy off snapshots of VCA for backup and thus may "share storage resources" with an EACMS? It is not clear where the scope of this "EACMS" ends. Southern believes there is clarity and simplicity for SCI that hosts a BCS and is in an ESP, but suggests scoping SCI to that which hosts a BCS and creating separate requirements to specifically address access to the mgt plane of an EACMS or PACS, for example (however, see Q14 as even that is problematic with the broadness of EACMS). This would be much more straightforward than treating SCI outside the ESP the same as SCI hosting a BCS.

Southern proposes the following alternative language for defining SCI, EACMS and PACS:

SCI: One or more programmable electronic devices, including the software and Management Interfaces, that share:

- CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA; or
- storage resources with any part of a BES Cyber System.

Each SCI is either:

- included in one or more BES Cyber Systems; or
- identified independently.

SCI does not include the supported VCA or CA with which it shares its resources.

EACMS: Cyber Assets or Virtual Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Intermediate Systems.

PACS: Cyber Assets or Virtual Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Likes 0	
Dislikes 0	

Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE

Answer	No
Document Name	

Comment

<duplicate>

Likes 0	
Dislikes 0	

Response

Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	
Eversource recommends using "Independently identified". The term seems inconsistent in regards to how its used in all the CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
While it is clear to those that have been following this project and or understand virtualization technologies and how it is used, a non-technical person may need more clarification. Further, “SCI identified independently…” the information provided in the most recent webinar was much clearer than what reads in the standards and Technical Rationale, but that is not binding. While both try to explain it, we don’t feel the Technical Rationale and glossary term does enough to distinguish exactly what is intended by the SDT. Secondly, CIP-002 R1.x doesn’t use the same verbiage. For example, “A XXXX impact BCS and independent SCI supporting any part of the XXXX impact BCS...” This should read: “A XXXX impact BCS and any SCI identified independently… supporting any part of the XXXX impact BCS...” We do feel these two classifications could work for industry, but need significant and binding definitions and distinctions with technical basis so entities can avoid misclassification of SCI.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	

Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
Requesting better clarification as industry may misinterpret especially the SCI “form” relationship to a function.	
Likes 0	
Dislikes 0	
Response	

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
The draft language is not clear. We assume that the phrase means SCI not declared as part of a BCA, PCA, EACMS, or PACS but it supports the BCA, PCA, EACMS, or PACS function (for example, a BCA can be run on VM system and the VM system will be defined as SCI, and the SCI can be declared as only SCI and not a dual declaration as a BCA and a SCI). However, this is only an assumption. How can SCI can both be independent and supporting any part of a BES Cyber System? If SCI supports any part of a BES Cyber System then it is not independent and is supporting.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Not clear on how the SCI is defined in this scenario. For the definition of "SCI identified indepently" is unclear what is meant by this definition, and is not clearly spelled out but an assumption is made. It appears to be assumed that the phrase means SCI not declared as part of a BCA, PCA, EACMS or PACS but it supports the BCA, PCA, EACMS, or PACS function. Would like this clearly spelled out by defintion and by each of the Applicable Systems column.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	No
Document Name	
Comment	
Additional guidance is needed for “SCI identified independently.” Also, the phrase “independent SCI supporting…” is not clear. Is this specifically to the VM environment used to create the virtual BCS?	

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	No
Document Name	

Comment

"SCI identified independently" is not clear and needs additional clarification.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

In support of IRC SRC/SWG.

This language can be misinterpreted. Recommend clarification. Current language is “SCI identified independently supporting an Applicable System.” Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Please provide additional clarification with respect to Applicable Systems callout for SCI beyond the phrase "SCI identified independently...".	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
Additional guidance is needed for “SCI identified independently.” Also, the phrase “independent SCI supporting…” is not clear. Is this specifically to the VM environment used to create the virtual BCS?	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	

Likes 0

Dislikes 0

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0

Dislikes 0

Response

Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5

Answer	No
Document Name	

Comment

Additional clarification is needed.

Recommend spelling out "Shared Cyber Infrastructure" and its acronym within the standard text.

Recommend including the definition within the text, or make a statement in the text directing to the definition in the definition list.

Likes 0

Dislikes 0

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The language “SCI identified independently” is not clear and should be removed from CIP-002 to CIP-013 (see our comments 1 in Q1). Resulting from our proposed changes to the definitions in Q1, the language “SCI identified independently” is no longer needed. A SCI should be identified either as one of the existing CIP cyber assets or out of CIP cyber asset scope.

This is not clear. We assume that the phrase means SCI not declared as part of a BCA, PCA, EACMS, or PACS but it supports the BCA, PCA, EACMS, or PACS function (for example, a BCA can be run on VM system and the VM system will be defined as SCI, and the SCI can be declared as only SCI and not a dual declaration as a BCA and a SCI). However, this is only an assumption.

Further, the phrase “independent SCI supporting any part of the … BCS” is confusing. It is not clear how an SCI can both be independent and supporting any part of a BES Cyber System. On its face it would seem that if an SCI supports any part of a BES Cyber System then it is not independent and is supporting.

We acknowledge the SDT’s attempt to avoid a “hall of mirrors” scenario where it could be interpreted that a device serving as an EACMS is required to have its own EACMS. However we also feel this situation may already occur today in some audits and not just a possibility going forward in the future. We recommend modifying existing definitions of BES Cyber System, BES Cyber Asset, and/or EACMS (ex. including an exclusionary phrase that an EACMS does not require its own EACMS).

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

This language can be misinterpreted. Recommend clarification. Current language is “SCI identified independently supporting an Applicable System.” Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

The context of the question isn’t clear is this question a general question or it’s pertaining to CIP-002.

Also, the question offers two choices; “Is this clear” or “is additional clarification needed” yet the choices are Yes/No.

So, our answer; is No, it’s not clear and yes additional clarification is needed.

Our hypothesis is that it must be a general question. We are not sure of the value of identifying the SCI (“supporting SCI” vs an “independent supporting SCI”), the SCI should be controlled and own requirements.

If the SDT maintains its distinction, they should enforce two types of categorizations and the requirements should be defined with those two types of categorizations in mind.

Likes 0	
Dislikes 0	

Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP fully supports EEI's comments that the process for the independent identification of Shared Cyber Infrastructure (SCI) is not clear and needs additional clarification.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
In support of NPCC RSC comments This language can be misinterpreted. Recommend clarification. Current language is "SCI identified independently supporting an Applicable System." Suggest adding a comma to distinguish between "identified independently" and "supporting." Resulting in "SCI identified independently, supporting an Applicable System"	

The context of the question isn’t clear is this question a general question or it’s pertaining to CIP-002.

Also, the question offers two choices; “Is this clear” or “is additional clarification needed” yet the choices are Yes/No.

So, our answer; is No, it’s not clear and yes additional clarification is needed.

Our hypothesis is that it must be a general question. We are not sure of the value of identifying the SCI (“supporting SCI” vs an “independent supporting SCI”), the SCI should be controlled and own requirements.

If the SDT maintains its distinction, they should enforce two types of categorizations and the requirements should be defined with those two types of categorizations in mind.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Additional guidance is needed for “SCI identified independently.” Also, the phrase “independent SCI supporting…” is not clear. Is this specifically to the VM environment used to create the virtual BCS?	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
If the language “SCI identifieid independently” is used then it would be beneficial for “identified independently” to be explicitly defined.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No

Document Name	
Comment	
We support NPCC TFIST's comments as found below: This language can be misinterpreted. Recommend clarification. Current language is “SCI identified independently supporting an Applicable System.” Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	No
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	

Answer	No
Document Name	

Comment

The definition of Shared Cyber Infrastructure (SCI) will be better explained with the term “SCI identified as supporting, but not part of…”.

BC Hydro requests that SDT provide more clarity around the concept of "not part of.." to better understand the separation point between whether an SCI is considered supporting but not actually part of BCAs, PCAs, EACMS or PACS.

BC Hydro also requests that SDT include a couple of practical examples to explain this concept within the Technical Rationale and proposed definition of SCI.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No
Document Name	

Comment

It is not clear what is meant by “SCI identified independently…”

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE finds the language “SCI identified independently supporting an Applicable System above” confusing. It is confusing because “SCI identified independently” is a process, and CIP-002-7 R1.1 uses the term “independent SCI” when it asks to identify, “A high impact BCS and independent SCI supporting …” When stated in this context, the phrase “independent SCI” is a thing that can be defined. SIGE proposes that the Applicable Systems column should state “Independent SCI that supports an Applicable System above” and that “independent SCI” can be defined or explained as “a Cyber System identified separately from the BCS, EACMS, PACS, and/or PCA it supports.”

Likes 0

Dislikes 0

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA does not support the definition and raises the question how SCI is to be identified independently. At there very least there would need to be guidance on what should be considered in the identification process.

Likes 0

Dislikes 0

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE finds the language “SCI identified independently supporting an Applicable System above” confusing.   It is confusing because “SCI identified independently” is a process, and CIP-002-7 R1.1 uses the term “independent SCI” when it asks to identify, “A high impact BCS and independent SCI supporting …” When stated in this context, the phrase “independent SCI” is a thing that can be defined. CEHE proposes that the Applicable Systems column should state “Independent SCI that supports an Applicable System above” and that “independent SCI” can be defined or explained as “a Cyber System identified separately from the BCS, EACMS, PACS, and/or PCA it supports.”

Likes 0

Dislikes 0

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Additional clarification is needed as “SCI identified independently…” remains ambiguous.

Likes 0

Dislikes 0

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer No

Document Name

Comment

The phrase “independent SCI supporting any part of the … BCS” is confusing. It is not clear how an SCI can both be independent and supporting any part of a BES Cyber System. On its face it would seem that if an SCI supports any part of a BES Cyber System then it is not independent and is supporting.

We acknowledge the SDT’s attempt to avoid a “hall of mirrors” scenario where it could be interpreted that a device serving as an EACMS is required to have its own EACMS. However we also feel this situation may already occur today in some audits and not just a possibility going forward in the future. We recommend modifying existing definitions of BES Cyber System, BES Cyber Asset, and/or EACMS (ex. including an exclusionary phrase that an EACMS does not require its own EACMS).

Likes 0

Dislikes 0

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer No

Document Name

Comment

While it is clear to those that have been following this project and or understand virtualization technologies and how it is used, a non-technical person may need more clarification. Further, “SCI identified independently…” the information provided in the most recent webinar was much clearer than what reads in the standards and Technical Rationale, but that is not binding. While both try to explain it, we don’t feel the Technical Rationale and glossary term does enough to distinguish exactly what is intended by the SDT.

Secondly, CIP-002 R1.x doesn’t use the same verbiage. For example, “A XXXX impact BCS and independent SCI supporting any part of the XXXX impact BCS...” This should read: “A XXXX impact BCS and any SCI identified independently… supporting any part of the XXXX impact BCS...”

We do feel these two classifications could work for industry, but need significant and binding definitions and distinctions with technical basis so entities can avoid misclassification of SCI.

AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Additional clarification is needed	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
The phrase “SCI Identified Indepedently, and more generally the desfinition of SCI is ambiguous and It is confusing to understand the definition of Shared Cyber Infrastrure (SCI) and therefore the overall requirement is unclear. Is SCI watermarked at the highest level? Strongly encourage better definition within the language of the standard and definitions to ensure that implementation is not dependent on independent on non-enforcable technical rationale and implementation guidelines.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	

AZPS feels that “SCI identified as supporting, but not part of” provides more clarity than “SCI identified independently…”, as it could be interpreted as applied to an SCI that is only supporting an applicable system. We feel the statement “SCI that supports an applicable system that is independently categorized as an SCI and as not part of the applicable BES Cyber System” provides more clarity.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
This is already clarified in the third and fourth bullet of the SCI definition. Suggest using ‘SCI supporting an Applicable System above.’ See (CIP-005-8 Part 1.5)	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
This is not clear. We assume that the phrase means SCI not declared as part of a BCA, PCA, EACMS, or PACS but it supports the BCA, PCA, EACMS, or PACS function (for example, a BCA can be run on VM system and the VM system will be defined as SCI, and the SCI can be declared as only SCI and not a dual declaration as a BCA and a SCI). However, this is only an assumption. Further, the phrase “independent SCI supporting any part of the … BCS” is confusing. It is not clear how an SCI can both be independent and supporting any part of a BES Cyber System. On its face it would seem that if an SCI supports any part of a BES Cyber System then it is not independent and is supporting. We acknowledge the SDT’s attempt to avoid a “hall of mirrors” scenario where it could be interpreted that a device serving as an EACMS is required to have its own EACMS. However we also feel this situation may already occur today in some audits and not just a possibility going forward in the future. We recommend modifying existing definitions of BES Cyber System, BES Cyber Asset, and/or EACMS (ex. including an exclusionary phrase that an EACMS does not require its own EACMS).	
Likes 0	

Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5

Answer	No
Document Name	

Comment

See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

Introduction of the SCI Group concept as enumerated in response to Question 1 would provide the further clarity needed to address the relationship of devices identified as SCI to the BCS or SCIG of which they are a member. This additional clarity should be reinforced in the definitions, proposed as follows:

DUKE ENERGY PROPOSED DEFINITIONS FOR BCS, SCI, and SCIG:

BES Cyber System (BCS) - One or more BES Cyber Assets logically grouped by a Responsible Entity to perform one or more reliability tasks for a functional entity, including Shared Cyber Infrastructure that the Responsible Entity chooses to group into the BES Cyber System it supports.

Shared Cyber Infrastructure (SCI) - Programmable electronic devices, including the software and Management Interfaces, that share…(proposed bullets remain)… Each SCI is grouped by the Responsible Entity into one or more BCS or SCIG. SCI does not include the supported VCA or CA with which it shares its resources.

Shared Cyber Infrastructure Group (SCIG) - One or more Shared Cyber Infrastructure devices logically grouped by a Responsible Entity.

Likes 0	
Dislikes 0	

Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Additional clarification is required. Some SCI may provide underlying compute, storage, or network virtualization services, which is essential for the proper function of a BCS. Other SCI systems such as those providing overlays for management functions or monitoring, may not be required for real-time BCS functionality. Accordingly, that distinction, and provision of controls accordingly, would be beneficial in the associated glossary terms.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
The Applicable System, “SCI identified independently” is ambiguous and unclear at best. Specifically, if SCI is hosting multiple Applicable Systems of different ratings, how is the SCI to be classified? Should it be high watermarked and protected to the highest rating of those Applicable Systems? If so, the SCI should be classified at the high watermark and be afforded the same protections as the Applicable System it supports - BCS, EACMS, PACS. The current definition and requirement is ambiguous which could result in an interpretation that applies BCS controls to an SCI that only supports EACMS or PACS. NRG requests the Standards Drafting Team provide more clarity between the two options: “All in” and “Identified SCI Option” as they seem to apply only when supporting a BCS and not in instances where SCI is hosting EACMS and/or PACS only. NRG disagrees with	

the Technical Rationale that requires logical isolation of SCI that hosts EACMS/PACS and no impact cyber systems. Within the context of the current CIP standards, there is no requirement for logical isolation between physical servers in this scenario.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

The Applicable System, “SCI identified independently” is ambiguous and unclear at best. Specifically, if SCI is hosting multiple Applicable Systems of different ratings, how is the SCI to be classified? Should it be high watermarked and protected to the highest rating of those Applicable Systems? If so, the SCI should be classified at the high watermark and be afforded the same protections as the Applicable System it supports - BCS, EACMS, PACS. The current definition and requirement is ambiguous which could result in an interpretation that applies BCS controls to an SCI that only supports EACMS or PACS. NRG requests the Standards Drafting Team provide more clarity between the two options: “All in” and “Identified SCI Option” as they seem to apply only when supporting a BCS and not in instances where SCI is hosting EACMS and/or PACS only. NRG disagrees with the Technical Rationale that requires logical isolation of SCI that hosts EACMS/PACS and no impact cyber systems. Within the context of the current CIP standards, there is no requirement for logical isolation between physical servers in this scenario.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	No
Document Name	

Comment

The term "SCI identified independently" does not read intuitively without reading the guidance and technical rationale. Since those documents are not auditable, it must stand on its own and needs more revision to be more clear. Consider developing an additional defined term and classification: "Independent SCI" - "An SCI that is not identified as part of a BCS or its associated EACMS, PACS, or PCAs." This approach would keep the requirement language clean and include the needed guidance in the auditable parts of the standards and definitions.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy recommends modifying the definition as folows: “SCI identified as supporting **the functionality,** but not part of…”.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
Reclamation recommends adding the additional clarification (such as “SCI identified as supporting, but not part of…”).	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes

Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Yes, it is clear that the “SCI identified independently” means that it is supporting any part of a high or medium impact BCS or associated EACMS, PACS or PCAs and is not included in the BCS. However, since “SCI identified independently…” is explicitly listed in the applicability columns, the other option for SCI to be included within the CIP System should also be explicitly stated. For example, “High Impact BCS, including supporting SCI, and their associated…”.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
: **GSOC recommends revising the language in the definition of SCI such that it is clear to registered entities that “Each SCI must be identified as either…” As well, when SCI is addressed within other definitions, requirements, or applicable systems columns, consistent language should be used throughout, i.e., within the body of the standards, within the definitions, and between the definitions and the standards. As an example of inconsistencies identified in the new definitions, SCI is characterized as “supporting,” “included in,” or “grouped in/with” in various definitions, which usage may not comport with the terms used in the definition of SCI. Additionally, in CIP-002, SCI is referenced as “supporting” or “independent supporting,” but the term “supporting” is not utilized in the definition of SCI nor in its potential charcterizations as set forth in the definition. Finally, SCI reference language included in CIP-006 and other standards, at times, includes a clarifications to ensure exclusion of those SCI grouped into a BCS, but that language is also not consistently applied throughout the standards. To ensure clarity, it is recommended that the language utilized to reference SCIs is consistent throughout the definitions, throughout the standards, and between the definitions and standards.**	
Likes 0	

Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Yes, although PNMR agrees with EEI that the term "independent SCI" should be clearly explained.	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Yes, this is clear.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

3. The SDT modified the ERC definition to reference “outside the asset containing”. This is to allow scoping based on connectivity of the logging systems as required by CIP-007 Requirement R4 as well as the scoping of requirement parts in CIP-004 and CIP-006 based on risk. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

There is insufficient clarity provided within the proposed terms to ensure consistent understanding and identification of applicable traffic.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy supports the comments of EEI.

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

Duke has identified three concerns with the proposed ERC definition and underlying strategy:

First, the “outside the asset containing” language expands the current ambiguity in CIP-003 to High and Medium sites, allowing for auditor interpretation with respect to how communication that is translated or terminated through a bastion host locally at the asset should be assessed. It is not clear from the definitions whether the SDT intends that communication from an outside location that first terminates on a non-CIP System at the asset and then pivots to a CIP System at the asset is included in this ERC definition, or if that break in communication is basis to exclude the CIP System from the ERC applicability.

Second, use of the ERC definition to attempt to address security concerns associated with remote access to devices that are accessible based on Serial to IP conversion alone exacerbates the CIP-004, 006, and 007 scoping challenges noted by the SDT.

The ERO has socialized a better path forward using the IRA definition to ensure that devices accessible in this manner are correctly secured. This would be a better strategy for securing these assets while minimizing low-value compliance paperwork (e.g. documenting lack of syslog capability on a serial-only relay). This change would take the SDT's removal of ERC from the CIP-005 requirement language to its logical conclusion, removing the dependence on the ERC definition to define security posture and instead using it as a scoping tool. Refer to slides 9-11 in following presentation: https://www.nerc.com/pa/Stand/Project%20201602%20Modifications%20to%20CIP%20Standards%20RF/2016-02_ERC_and_IRA_Webinar_Slides_05072020.pdf

Third, the use of CIP Systems creates confusion as there are no ERC requirements applied to other classifications of devices that are included in the CIP Systems definition (e.g. EACMS, PACS, and TCA devices). Although simplicity in definitions is desirable, it would be clearer to spell out the system types that are relevant to the defined term (e.g. BCS, PCA, SCI).

Therefore, Duke proposes the following definition of ERC, which incorporates the SDT's improved "communicate" terminology while remaining focused on the ESP boundary as the point where the determination is made.

External Routable Connectivity (ERC) - The ability to communicate across a defined ESP via a bi-directional routable protocol connection.

It does not appear that the SDT's rationale regarding the shrinkage of the ESP in Zero Trust environments is likely to reach the intra-device level given that the CA, VCA, and SCI definitions remain device-centric. Therefore, Duke strongly feels that the fundamental change proposed by the SDT is not justified by the potential downside the SDT has identified.

Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Just as it has been problematic for entities with assets containing low impact BES Cyber Systems to identify where electronic access controls must be afforded for routable protocol, the use of a physical construct for where logical controls are implemented for CIP-004 and CIP-006 appears to further the problem. Consider the following two edit to the proposed ERC definition: The ability to communicate to a CIP System using a bi-directional routable protocol from a nonCIP System.	
Likes 0	
Dislikes 0	
Response	

William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
The lower-case ‘asset’ used in the definition really erodes the intent of ERC. This could allow an entity to not consider communication between corporate networks and BCS to be ERC if they are in the same building (‘asset’), for example at a Control Center. Alternative proposal: *The ability to communicate to a CIP System using a bi-directional routable protocol from a Cyber System that is not protected by an Electronic Security Perimeter located at the same asset. However, the alternate proposal still has a limitation on ‘asset’, which is an undefined term.*	
Likes 0	
Dislikes 0	
Response	

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS feels that changing the language to “communicate to” instead of “accessing” has the potential to expand the scope of ERC unintentionally. Including “outside the asset containing the CIP system” leads to ambiguity while use of ESP helps clarify intent. The new definition suits virtual fully, but leaves vagueness and abiguity to physical aspects. AZPS respectfully recommends creating two separate definitions for physical and virtual.	

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	No
Document Name	

Comment

The new language does not clarify where the border where bi-directional communication is considered. The current definition, which specifies the border to be at that EACMS (local firewall) is adequate for most cases. We understand that the definition needs to be adjusted to recognize implementation of zero trust models. However, clarifying that external routable connectivity is determined at the physical border of the asset would clearly identify where external routable connectivity is to be considered.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Additional clarification is needed

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

ACES does not agree with the reference “outside the asset containing” as a scoping mechanism for CIP-007 R4. We do not understand the correlation of ERC to CIP-007 logging or CIP-004 and CIP-006 risks. Using the “asset” as a scoping mechanism could lead to various interpretations and allow for loop holes for access. In our opinion, “outside the asset containing” is not necessary to define ERC. We feel ESP is still the proper scoping mechanism.

AEPC has signed on to ACES comments.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE does not agree with the proposed change to the ERC definition because the phrase “from outside the asset containing the CIP System” is not clear. “Asset” is not a term in the NERC Glossary of Terms; therefore the definition cannot clarify precisely what “outside the asset” means. Is it a room, building, geographical location, or something else?

In addition, the proposed definition greatly expands the existing definition by changing from “BES Cyber System” to “CIP System” and by changing from “... to access …” to “… to communicate …”. However, this expansion can be controlled by specifying specific Cyber Systems in the requirements.

CEHE suggests maintaining the currently approved definition until a more clearly defined proposal is offered or “Asset” is added as a defined term in the NERC Glossary.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA does not support the phrase “outside the asset” is vague and confusing. NCPA suggests the change “…ability to communicate to a CIP System using bi-directional routable protocol from a separate asset containing the CIP system.”

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE does not agree with the proposed change to the ERC definition because the phrase “from outside the asset containing the CIP System” is not clear. “Asset” is not a term in the NERC Glossary of Terms; therefore the definition cannot clarify precisely what “outside the asset” means. Is it a room, building, geographical location, or something else?

In addition, the proposed definition greatly expands the existing definition by changing from “BES Cyber System” to “CIP System” and by changing from “... to access …” to “… to communicate …”. However, this expansion can be controlled by specifying specific Cyber Systems in the requirements.

SIGE suggests maintaining the currently approved definition until a more clearly defined proposal is offered or “Asset” is added as a defined term in the NERC Glossary.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No
Document Name	

Comment

It’s not clear what is meant by the phrase “from outside the asset containing the CIP System.” This makes it sound like all CIP Systems must reside within a electronic security perimeter. It is unclear what it is that the SDT is attempting to accomplish with this wording or how it is allowing scoping based on connectivity of the logging systems as required by CIP-007. Further, the use of the term “asset,” with a lower case A, often causes confusion with “Cyber Asset” when discussing requirements with SMEs.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No

Document Name	
Comment	

Texas RE is concerned the new proposed changes to the ERC definition only focus on WAN and excludes LAN network communications. LAN and WAN network communications are both captured under the current definition. If the proposed changes are approved, registered entities could potentially argue that they have no ERC even though a bi-directional routable protocol connection is being utilized from LAN to LAN.

As such, this change could reduce the entities' overall security posture by placing such communications potentially outside the scope of the entities' CIP-program. For example, the proposed language for CIP-005 R2.1 includes in scope "medium impact BCS with ERC". Since the proposed ERC definition focuses on the term "asset", Texas RE is concerned that entities could potentially read the "asset" language to remove from scope BCAs such as operator consoles that are not accessible from outside the Control Center (that is, from outside the "asset"). Specifically, because there is no ERC from outside of the Control Center, it could be argued that the operator consoles no longer fall within the proposed ERC definition. As a result, important CIP protections such as the use of an Intermediate System to access those assets, physical protections, and personnel training requirements would be limited.

Given these concerns, Texas RE recommends retaining the current definition of ERC.

Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	
Comment	

BC Hydro seeks more clarity on the term "asset" in relation to the reference "outside the asset containing." Specifically, it is not clear whether the term "asset" is meant to talk to individual BES Elements (i.e. a specific transformer, circuit breaker, etc.) or whether entities are given the latitude to define the boundaries of assets (i.e. could be based on defined physical boundaries of a broader transmission or generation station or a Control Centre). Recommend providing specific drawing examples similar to the models provided under the CIP-003-8 standard to help visualize through practical network architecture to characterize what would constitute ERC under this new proposed definition.

Likes 0	
Dislikes 0	
Response	

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No

Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	No
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We support NPCC TFIST's comments as found below: We understand that “outside the asset containing” is a scoping mechanism. Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset not the ESP. Did the SDT intend this implicit requirement? We are confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary? Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. ERC means external to what?	
Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

The modification to the definition to ERC brings serially connected OT Devices using a protocol-converter into scope for multiple CIP-007 requirements. In some instances, compliance with all CIP-007 requirements would be impossible. The use of a protocol converter does not facilitate centralized logging, review, and alarming (based on events). It simply facilitates data acquisition and IRA to these devices. We suggest not revising the definition of ERC, leaving the concept of a protocol break in place and require the protocol converter to either be categorized as a BCA, PCA or EACMS (depending on the circumstance). The serial OT device could still utilize the proposed definition for IRA to be in scope for CIP-005.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

OKGE supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

The proposed change to the ERC definition expands scope by making the boundary physical “asset” from the original electronic concept. ERC could happen within a room where two systems have discrete ESPs that communicate between each other.

Change the ability to “access” to “communicate to” to bring the connectivity rationale into the term.

Suggested definition - *The ability to communicate to a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.*	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
In support of NPCC RSC comments.	

We understand that “outside the asset containing” is a scoping mechanism.

Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset not the ESP. Did the SDT intend this implicit requirement?

We are confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary?

Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. ERC means external to what?

The overall definition of ERC is

The ability to communicate to a CIP System using a bi-directional routable protocol from outside the asset containing the CIP System.

(The definition of CIP System is included for precision)

The ability to communicate to a CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.) using a bi-directional routable protocol from outside the asset containing the CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.).

We don’t see the added value of this “scoping” for CIP-007 R4, CIP-004, CIP-006. This definition includes additional asset types (EACMS, PACS, SCI, PCA, TCA) to the concept of ERC. One could think that future requirements could come forward, like for EACMS with ERC or even TCA with ERC, but it’s not the case.

In reference to CIP-007 R4, the text used is the following

Medium Impact BCS with External Routable Connectivity and their associated:

1. EACMS;

2. PACS; and

3. PCA

SCI identified independently supporting an Applicable System above

The ERC trigger is still based on the BCS.

If the understanding of asset (“the asset containing “) is equivalent to the following … i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. RAS that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above… the suggested definition is interesting.

Our comprehension is that if we have two HIGH/Medium-Impact BCS in the same Control Center (asset) using a bi-directional routable protocol to establish their communication and that any of those BCS doesn’t use a bi-directional routable protocol outside of the Control Center, the ERC definition wouldn’t be applied. Furthermore, if any of those two BCS would be using a bi-directional routable protocol outside of the asset of both BCS would be tagged as being ERC.

We suggest the removal of CIP System in the definition.

Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP does not support the proposed changes to the External Routable Connectivity (ERC) definition and is in support of EEI's comments. The new definition for ERC expands the scope by (1) replacing the defined term "BES Cyber System (BCS)" with a proposed new term "CIP System", and (2) changing "the ability to access …" to "the ability to communicate to …". In addition, AEP seeks additional clarification on "asset containing the CIP System". The term "asset" could be interpreted in many ways and could be a point of contention if an entity identified an "asset" at a fence line where an auditor may have a different opinion on where that line of demarcation for an "asset" might be drawn.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
We understand that "outside the asset containing" is a scoping mechanism.	

Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset not the ESP. Did the SDT intend this implicit requirement?

We are confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary?

Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. ERC means external to what?

The overall definition of ERC is

The ability to communicate to a CIP System using a bi-directional routable protocol from outside the asset containing the CIP System.

(The definition of CIP System is included for precision)

The ability to communicate to a CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.) using a bi-directional routable protocol from outside the asset containing the CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.).

We don’t see the added value of this “scoping” for CIP-007 R4, CIP-004, CIP-006. This definition includes additional asset types (EACMS, PACS, SCI, PCA, TCA) to the concept of ERC. One could think that future requirements could come forward, like for EACMS with ERC or even TCA with ERC, but it’s not the case.

In reference to CIP-007 R4, the text used is the following

Medium Impact BCS with External Routable Connectivity and their associated:

1. EACMS;

2. PACS; and

3. PCA

SCI identified independently supporting an Applicable System above

The ERC trigger is still based on the BCS.

If the understanding of asset (“the asset containing “) is equivalent to the following … i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. RAS that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above… the suggested definition is interesting.

Our comprehension is that if we have two HIGH/Medium-Impact BCS in the same Control Center (asset) using a bi-directional routable protocol to establish their communication and that any of those BCS doesn’t use a bi-directional routable protocol outside of the Control Center, the ERC definition wouldn’t be applied. Furthermore, if any of those two BCS would be using a bi-directional routable protocol outside of the asset of both BCS would be tagged as being ERC.

We suggest the removal of CIP System in the definition.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

We disagree to modifying ERC definition. Given that the ESP is still effective and the language BCS with ERC and IRA are still used by STD in the revised requirements, ERC should be still ESP and BCS based rather than asset based. If using the physical boundary to identify ERC, it is hard to decide which BCS with ERC and which BCS without ERC, which would cause ERC identification issues and various interpretations. Also the asset boundary will cause the security risk since the highwater marking wouldn't apply within a physical boundary. Furthermore, physical boundary would cause audit issue since it is not a defined term. For instance, whether a generating station power house and its switchyard are treated as the same asset or separate asset will get the different results. In addition, the proposed ERC definition overreaches the goal of SAR since the revised ERC refers to CIP System which includes all types of CIP cyber assets. The SRA doesn't require entities to identify ERC for EACMS, PACS, and TCA that are outside ESP.

Recommendation: Restore the current ERC definition since it still fits the revised requirements.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

The proposed change to the ERC definition expands scope by making the boundary physical "asset" from the original electronic concept. ERC could happen within a room where two systems have discrete ESPs that communicate between each other.

Change the ability to "access" to "communicate to" to bring the connectivity rationale into the term.

Suggested definition - *The ability to communicate to a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.*

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

In support of IRC SRC/SWG.

We understand that “outside the asset containing” is a scoping mechanism.

Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset not the ESP. Did the SDT intend this implicit requirement?

We are confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary?

Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. ERC means external to what?

Likes 0

Dislikes 0

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	No
Document Name	

Comment

The proposed change to the ERC definition expands scope by making the boundary physical “asset” from the original electronic concept. ERC could happen within a room where two systems have discrete ESPs that communicate with each other.

Change the ability to “access” to “communicate to” to bring the connectivity rationale into the term.

Suggested definition - *The ability to communicate to a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.*

Likes 0

Dislikes 0

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

We support EEI's comments on this question.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Because the term and concept of ESP remains effective and the BCS language of ERC and IRA are used by STD in the revised requirements, ERC should remain ESP and BCS based rather than asset based. It is difficult to determine which BCS with ERC and which BCS without ERC would apply with the proposed language.

The asset boundary will cause a security risk since the highwater marking wouldn't apply within a physical boundary. Furthermore, physical boundary would cause audit issue since it is not a defined term. For instance, whether a generating station power house and its switchyard are treated as the same asset or separate asset will get the different results. In addition, the proposed ERC definition overreaches the goal of SAR since the revised ERC refers to CIP System which includes all types of CIP cyber assets. The SRA doesn't require entities to identify ERC for EACMS, PACS, and TCA that are outside ESP.

Recommendation: Restore the current ERC definition since it still fits the revised requirements.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- The proposed change for ERC is confusing, including March and August discussions with the SDT during outreach, for when a CIP System that serial converts RS-232 or RS-485 may extend ERC beyond the ESP to medium impact BCAs, PCAs and Non-CIP Cyber Asset. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation.
    - Where is the electronic boundary and how does it apply when not routable?
    - Where is the physical boundary when serial extends out of the substation to field devices?
    - When does ERC apply to a CIP System that is connected serially that was previously consider non-routable before the new proposed updates from Project 2016-02 SDT?
        - Please clarify the language that extends applicability to a CIP System using serial communication within the asset/site?

    - If the serial link can change the configuration of a BCA is the SDT intending Entities now have a BCA with ERC when previously the demarcation was the serial link?

- Please clarify how ERC is applied to standards when an SCI EACMS in a Medium Impact substation that provides conversion of ERC to serial for remote configuration support of RTU and Relays rated as Medium BCA along with Relays that are Low Impact BCA and Non-CIP System Relays how ERC is being applied when using serial communication has the proposed standard requirements intended that PSP and 15 month password changes now apply?

- Will applicability today for BCA with ERC apply going forward with the new proposed definitions and requirements to a BCS Medium Impact Relay connected serially that is being managed through RS-232?

- Does a Non-CIP System distribution Relay now become a PCA because it is connected to the Medium Impact Serial converter?

- The SDT ERC changes appears to be impacting the BROS process may require improved language in CIP-002 Attachment 1 as it cascades into other standards applicability requiring clarification:

    - CIP-002 R1 and R2 - Would Entities now need to identify BCA's that are serially connected and update CIP-002 BCS List to show these now as part of either SCADA or Protection with ERC?

    - CIP-004 R4.3 – Would electronic access to devices with ERC now be an entitlement to be mapped all serially connected devices requiring and role authorization?

    - CIP-005 R1.1 – Does the SDT expect that the ESP diagrams to now show serially connected devices within the substation house PSP and cables external out of the PSP to the devices in the structure including Transformers, CAP Banks, etc?

    - CIP-006 R1.2, 1.4, 1.7, 1.8, 1.9, 2.2, 2.3, 3.1 – Does the SDT intend that devices without ERC currently are outside a PSP (allowed by CIP-006 R1.1) will now with the proposed changes require the establishment of a PSP, with control, alerting, response, logging, visitor escort and system testing for serially connected IED in transformer cabinet for temperature monitoring, metering devices or other IEDs outside of the Station House PSP?

    - CIP-007 R1 – Please confirm the P1.1 Logical ports justification and details for serially connected CIP Systems are excluded but expectation of the physical wiring will be required for P1.2?

    - CIP-007 R4.2 – Please clarify the serial CIP System must now alert for failure of event logging.

    - CIP-007 R5.6 – Please clarify a serial CIP System such as an RTU or Relay that was a BCA or PCA without ERC now with the proposed change requires the password change every 15 months?

    - CIP-010 R1.1.4 – How will an Entity meet the baseline requirement for logical port open on each serially connected device or can a by device capability exclusion apply?

    - CIP-010 R1.2, 3, 4 – Do the proposed update require all the change management sub-requirements apply when a device is serially connected/disconnected to a network or moved within a network while still a serial device?

    - CIP-010 R3 – Please confirm the annual CVA including network discovery will require serial communication assessments throughout the site/facility/asset?

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No

Document Name	
Comment	
ACES does not agree with the reference “outside the asset containing” as a scoping mechanism for CIP-007 R4. We do not understand the correlation of ERC to CIP-007 logging or CIP-004 and CIP-006 risks. Using the “asset” as a scoping mechanism could lead to various interpretations and allow for loop holes for access. In our opinion, “outside the asset containing” is not necessary to define ERC. We feel ESP is still the proper scoping mechanism.	
Likes 0	
Dislikes 0	
Response	
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	
Eversource recommends clarification regarding what "outside the asset containing" is clarifying.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA is concerned with bringing serial devices into scope as part of ‘Applicable System with ERC’. This would require the serial relays to comply with additional CIP requirements. Expanding the scope of ERC to serial-based devices could significantly increase implementation cost and require new tools/products to help with ensuring compliance. The changes needed to enforce Physical Security requirement CIP-006 R1.2 will require long lead times to implement especially for shared control houses.	
Likes 0	
Dislikes 0	
Response	
Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	

Answer	No
Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern agrees with the concept but does not agree with the proposed language. “Asset” should be better defined as it is too ambiguous and many requirements’ scoping is based on clarity around ERC. Additionally, ERC has changed from being defined in terms of a BCS to a ‘CIP System’ which includes all named types of devices. If a BCS inside an “asset” is isolated, however there is a docked TCA on another network inside the 'asset', does the BCS inherit ERC because a “CIP System” can be accessed in the asset? As the boundary broadens and the target is any CIP System, it has lost focus on the ability to externally communicate with a BCS. Southern suggests that ERC be defined in terms of the BCS, not the overly broad “CIP System”.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
LCRA is concerned with bringing serial devices into scope as part of ‘Applicable System with ERC’. This would require the serial relays to comply with additional CIP requirements. Expanding the scope of ERC to serial-based devices could significantly increase implementation cost and require new tools/products to help with ensuring compliance. The changes needed to enforce Physical Security requirement CIP-006 R1.2 will require long lead times to implement especially for shared control houses.	
Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT supports the IRC SRC comments and offers this additional comment:

- The proposed modification greatly expands the scope of the definition. “Asset” has historically referred to things like transmission, generation, etc. Before, ERC was limited to just BES Cyber System. Why is this needed with assets and systems that reside outside of an ESP? The definition also needs to accommodate technologies that do not use a routable protocol.

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC supports the SDT’s intentions, however the proposed draft language is still somewhat unclear. For those reasons, ATC requests consideration of clearer language and perhaps supporting diagrams. One example of a question we’ve asked ourselves was: If you connect from a router (EACMS) to talk to a switch would that be ERC? Also, If my Control Center “asset” has several rooms and various subnets, and some devices are on a non-BCS subnet but still physically inside the “asset” containing the BCS, shouldn’t a routable connection from that device to a BCA be considered ERC?

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI does not support the proposed change to the ERC definition because it expands the current definition by replacing the defined term BES Cyber System (BCS) with newly defined term “CIP System” and by changing from “... to access …” to “… to communicate …”. “Access” means the ability to make use of information (see NIST definition of access - https://csrc.nist.gov/glossary/term/access), while the term communicate has a much broader meaning and could be interpreted to mean that the act or ability to ping a device is now in scope.

Additionally, the use of the term “asset” within the context of the ERC definition raises potential compliance ambiguity and lack of uniformity that could result in different interpretations during an audit. To address these concerns, we offer the following:

The ability to access a BCS using a bidirectional routable protocol from outside the ESP that controls access to the BCS.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

This is a substantial change to the definition of ERC that has a larger impact than in the context of addressing virtualized environments.

This is a large change to bring into scope assets that are protected by the ESPs in the past but did not have to meet ERC requirement since this connection did not enable IRA.

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
The proposed change to the ERC definition expands scope by making the boundary physical “asset” from the original electronic concept. ERC could happen within a room where two systems have discrete ESPs that communicate between each other. Change the ability to “access” to “communicate to” to bring the connectivity rationale into the term. Suggested definition - *The ability to communicate to a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.*	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

We understand that “outside the asset containing” is a scoping mechanism.

Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset not the ESP. Did the SDT intend this implicit requirement?

We are confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary?

Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. ERC means external to what?

The overall definition of ERC is

The ability to communicate to a CIP System using a bi-directional routable protocol from outside the asset containing the CIP System.

(The definition of CIP System is included for precision)

The ability to communicate to a CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.) using a bi-directional routable protocol from outside the asset containing the CIP System (A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.).

We don’t see the added value of this “scoping” for CIP-007 R4, CIP-004, CIP-006. This definition includes additional asset types (EACMS, PACS, SCI, PCA, TCA) to the concept of ERC. One could think that future requirements could come forward, like for EACMS with ERC or even TCA with ERC, but it’s not the case.

In reference to CIP-007 R4, the text used is the following

Medium Impact BCS with External Routable Connectivity and their associated:

1. EACMS;

2. PACS; and

3. PCA

SCI identified independently supporting an Applicable System above

The ERC trigger is still based on the BCS.

If the understanding of asset (“the asset containing “) is equivalent to the following … i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. RAS that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above… the suggested definition is interesting.

Our comprehension is that if we have two HIGH/Medium-Impact BCS in the same Control Center (asset) using a bi-directional routable protocol to establish their communication and that any of those BCS doesn’t use a bi-directional routable protocol outside of the Control Center, the ERC definition

wouldn't be applied. Furthermore, if any of those two BCS would be using a bi-directional routable protocol outside of the asset of both BCS would be tagged as being ERC. We suggest the removal of CIP System in the definition.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST assumes this proposed revision is intended to bring into scope remote connections to serially-connected CIP Systems that traverse wide-area connections via TCP/IP before being converted, "locally," to serial. However, as written, it would exclude end-to-end routable connections from non-CIP Systems to CIP Systems established within a given asset (example: TCP/IP connection from a PC on corporate network to a CIP server in the same building behind an ESP on a CIP network). One loophole closed, another opened. N&ST believes the SDT should be able to address this problem by expanding the definition of ERC using an "either/or" format. ERC is either: "The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated ESP via a bi-directional routable protocol connection; or "The ability to communicate to a serially-connected CIP System using a bi-directional routable protocol from outside the asset containing the CIP System."	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

The IRC SRC understands “outside the asset containing” to be a scoping mechanism.

Request clarification. This new language creates an implicit requirement that the trust boundary is now at the asset and not the ESP. Is this understanding correct?

The IRC SRC is confused by the proposed change. We do not understand the trust boundary change from ESP to asset. Request clarification of demarcation. Where is the electronic boundary? Where is the physical boundary?

Given this update, we believe the Medium Impact boundary is not as well defined as the Low Impact boundary. External Routable Connectivity (ERC) now means external to what?

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	Yes
Document Name	

Comment

Dominion Energy agrees with the reason for the reference “outside the asset containing…” but the definition itself does not help determine if ERC exists within a communication link that involves a routable protocol that is converted to serial protocol at the last leg of the link. However, based on the NERC SDT Webinar, presented on August 4, it appears that ERC exists in this kind of communication. One or more high level reference diagrams that illustrate the general concept of the modified term ERC, or some examples of the concept, in an Implementation Guidance document would be beneficial. See also response to #14A below.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	Yes
Document Name	

Comment

Chelan agrees with the proposed definition changes for ERC.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	Yes
Document Name	

Comment

As long as ERC is not used instead of IRA. PNMR supports EEIs suggested definition of ERC.

Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE does not have MEDIUM impact BCS cases and thus no cases for which the ERC definition would affect scope for requirements.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Agree with change to ERC definition.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
While GSOC agrees with the intent of the change, it cannot support the proposed change as use of the generic term "asset" could cause confusion and inconsistency regarding the meaning of the term "asset" and its use across the body of standards. As an example, asset is utilized in CIP-002 and is meant to convey a physical facility or building. The generic use of "asset" within the new definition of ERC could, therefore, also be construed as referring to the physical building or facility in which a system is located, which is likely not the intended or	

only meaning. To reduce the potential for confusion, GSOC recommends that clarification be added to the definition of ‘ERC’ to ensure that the full intent and meaning of the term “asset” as used within the definition of ERC is clear and easily, consistently understood.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Yes, we argree with the proposed change because the language “through an EACMS controlling communications...” allows non-perimeter-based models of ERC including zero-trust.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	

4. The SDT proposes that the modified ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST believes the “routable protocol” qualifier should be retained:

“A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.”

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	

Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We suggest adding “routable protocol” to the revised definition. We feel this can still be used for both types of networks. We also suggest removing “CIP Systems,”and replace with “BES Cyber Systems.” Remove “enforced by an EACMS.” Suggested definition - *A set of configurations or policies [delete - enforced by an EACMS] that controls routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber Systems of the same impact rating and their associated PCA.*	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI agrees that the modified ESP definition can be used for both types of networks but seeks clarification regarding the inclusion of the phrase “and their associated PCAs”, which appears to be redundant to the second sentence in the definition. EEI notes that within the definition of CIP System, PCAs are clearly identified as a CIP System. We suggest the following as one possible solution: “A set of configurations or policies enforced by an EACMS that control routable protocol communications to or from any part of a BES Cyber System (BCS) and that groups BCS of the same impact rating.”	

Alternatively, the SDT might consider leveraging the defined term “Electronic Access Point (EAP)” rather than modifying the term ESP.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
The phrase "control communication" is too broad; it could include any policy/configuration that configures anything that communicates (e.g., an internal API within an application). The definition needs additional clarity such that an ESP is in the networking realm and is controlling the ability to deliver packets to a BCS on the network, which we gather is the intent since host-based firewalls are excluded. We suggest modifying it to "control routable protocol communication" to clarify that an ESP is a network level construct (even in zero trust) concerned with delivery of packets. The grouping statement in the ESP definition is confusing as it switches to "CIP Systems" and only BCS have impact ratings. Suggest changing this to "These configurations or policies group BES Cyber Systems of the same impact rating with their associated PCAs". In addition, we believe this sentence is attempting to say the ESP is the ‘innermost’ policy or configuration controlling access to the BCS and therefore grouping BCS of like impact rating and their PCAs. We suggest making further clarifications to that end. An enterprise’s Internet facing firewalls play some role in ‘controlling communications’ to eventual groups of BCS that may be many network zones deep behind many firewalls that are not the CIP-005 ESP of today. However, there appears to be nothing in the definition or CIP-005 R1.1 that clearly states the ESP in question is the layer of segmentation/isolation method immediately ‘outside’ the BCS.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	
The SDT is using the update to the definition as a mechanism to support zero-trust models, but the existing ESP definition does not preclude a Responsible Entity from applying the concept of zero-trust to its environment(s) in addition to its traditional ESP. The proposed modification does not obligate a Responsible Entity to adopt additional security controls. The statement in the Definitions and Exemptions Technical Rationale, “[i]n these models, the perimeter shrinks to increasingly more granular levels, potentially down to a process or resource level on a BCS and nothing on the network is trusted for unrestricted communications,” could be	

interpreted as meaning that traditional ESP-based perimeter security is not necessary or required. A Responsible Entity may choose to adopt a traditional ESP model, or a zero-trust model, without considering the benefits of a defense-in-depth approach that leverages both traditional perimeter-based security and zero-trust concepts.

AWS proposes the following language, “The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol that includes a set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.”

Detailed implementation guidance is necessary to support zero-trust and hybrid approaches.

Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No

Document Name

Comment

Relative to the definition of ESP, GSOC is concerned that the second sentence proposed in the new definition is unnecessary and could cause confusion regarding its applicability beyond a virtualized environment. In particular, use of the term “group” could connote actions or protections beyond the traditional and intended meaning of ESP. As well, the second sentence appears to act as an additional requirement on the use of ESPs that would be better suited for inclusion in the actual requirements as set forth in CIP-005-8. GSOC recommends deleting the second sentence from the definition and re-capturing the concept (as applicable) in the language of CIP-005-8.

GSOC requests the addition of clarifying language in CIP-005-8 R1.2 that would reinforce the approach of utilizing a traditional approach to electronic security perimeters in addition to the language proposed “EACMS that enforces an ESP for the Applicable System…” Current proposed language could be interpreted to only apply to communications traversing an EACMS enforcing an ESP in a virtualized environment, without providing for requirements concerning the same traffic traversing a traditional ESP such as a firewall or similar device.

Likes 0

Dislikes 0

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer No

Document Name

Comment

The modified ESP definition does not resolve the traditional firewall based network or future networks. The virtualization zero trust topology is underneath the ESP network and is a non-ESP model. It is configured in the virtualization layer prior to VCAs reaching the ESP network. IRA cannot be identified without an ESP boundary being defined since IRA is initiated outside ESP. Furthermore, the SDT proposed ESP definition would include routable and non-routable BCAs in which it overreaches the goal of SAR. In our view, the EAP is still effective for the ESP model to control communications to and from BCS using routable protocol inside an ESP. We recommend adding an alternative requirement in CIP-005 R1.1 to address the zero-trust model in which the ESP model is not used rather than revising ESP definition. Our proposed changes won’t affect the existing ESP definition and ESP related requirements while still addressing virtualization to meet the goal of SAR.

Recommendations:

1. Restore the current ESP definition since it is still effective for the perimeter-based routable network protection.
2. We propose the following changes for CIP-005 R1.1:
    i. All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP where all External Routable Connectivity must be through an identified EAP that permits only needed inbound and outbound access and denies all other access by default including the reason for granting access, or
    ii. All BCAs connected to a network via a routable external protocol shall through an EACMS that controls all communications to and from BCAs unless ESP model is used.

    We agree that the proposed ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. However, the routable protocol qualifier was removed and the new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. This seems like a circular definition. Also, it is our understanding that the SDT does not intend to have requirements baked into definitions but with the proposed ESP definition, and changes to CIP-005, the definition is the only place EACMS are required. We propose the following changes:

ESP definition: A set of configurations or policies that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

New CIP-005-X R1 Part 1.X:

Applicable Systems

High Impact BES Cyber Systems and their associated PCA

Medium Impact BES Cyber Systems and their associated PCA

Requirements

1.X.1 - EACMSs must be implemented to enforce ESPs where communication leaves the ESP, or where SCI is used.

1.X.2 - EAPs must be identified for ESPs.

When the proposed ESP definition is applied in the proposed CIP-005-X R1 Part 1.1 there is another issue since the definition no longer has the routable protocol qualifier. See our response to Question #10 below for further explanation.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

In our opinion it should be clarified that a BCA or PCA controlling access only to itself (such as a host-based firewall) does not qualify as an EACMS and likewise does not constitue an ESP, except in cases where zero-trust is being used in place of a traditional EACMS and Access Point (such as a firewall). We also support EEI's comments on this question.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment	

Suggesting that the SD go back and make modifications to the definitions. We agree that the proposed ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. However, the routable protocol qualifier was removed and the new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. This seems like a circular definition. Also, it is our understanding that the SDT does not intend to have requirements baked into definitions but with the proposed ESP definition, and changes to CIP-005, the definition is the only place EACMS are required. We propose the following changes:

ESP definition: A set of configurations or policies that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

New CIP-005-X R1 Part 1.X:

Applicable Systems

High Impact BES Cyber Systems and their associated PCA

Medium Impact BES Cyber Systems and their associated PCA

Requirements

1.X.1 - EACMSs must be implemented to enforce ESPs where communication leaves the ESP, or where SCI is used.

1.X.2 - EAPs must be identified for ESPs.

When the proposed ESP definition is applied in the proposed CIP-005-X R1 Part 1.1 there is another issue since the definition no longer has the routable protocol qualifier.

Likes 0	
Dislikes 0	

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	No
Document Name	

Comment

We suggest adding “routable protocol” to the revised definition. We feel this can still be used for both types of networks. We also suggest removing “CIP Systems,” and replace with “BES Cyber Systems.” Remove “enforced by an EACMS.”

Suggested definition - *A set of configurations or policies [delete - enforced by an EACMS] that controls routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber Systems of the same impact rating and their associated PCA.*

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3	
Answer	No
Document Name	
Comment	
GRE agrees with the comments submitted by the NSRF.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
While the modified ESP definition is a definite improvement with respect to support for future development of zero trust networking adoption, the measures associated with proposed CIP-005-8 R1 include specification of business reasons associated with the configuration identified in the definition. ISO-NE requests that the definition be updated to include the business reasons as a part of the ESP to clarify the relationship and the requirement to include such in the configuration and documentation related to ESP's.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
We suggest adding “routable protocol” to the revised definition. We feel this can still be used for both types of networks. We also suggest removing “CIP Systems,”and replace with “BES Cyber Systems.” Remove “enforced by an EACMS.” Suggested definition - *A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber Systems of the same impact rating and their associated PCA.*	
Likes 0	

Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We disagree with the modified ESP definition as it cannot resolve the traditional firewall based network and the future networks. The virtualization zero trust topology is underneath the ESP network and is a non-ESP model. It is configured in the virtualization layer prior to VCAs reaching the ESP network. Also, IRA cannot be identified without ESP boundary being defined since IRA is initiated outside ESP. Furthermore, the SDT proposed ESP definition would include routable and non-routable BCAs in which it overreaches the goal of SAR. In our view, the EAP is still effective for the ESP model to control communications to and from BCS using routable protocol inside an ESP. We recommend adding an alternative requirement in CIP-005	

R1.1 to address the zero-trust model in which the ESP model is not used rather than revising ESP definition. Our proposed changes won't affect the existing ESP definition and ESP related requirements while still addressing virtualization to meet the goal of SAR.

Recommendations:

1. Restore the current ESP definition since it is still effective for the perimeter-based routable network protection.

2. We propose the following changes for CIP-005 R1.1:

a. All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP where all External Routable Connectivity must be through an identified EAP that permits only needed inbound and outbound access and denies all other access by default including the reason for granting access, or

b. All BCAs connected to a network via a routable protocol shall through an EACMS that controls all communications to and from BCAs unless ESP model is used.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

While AEP agrees that the modified Electronic Security Perimeter (ESP) definition can be used for both type of networks (i.e., traditional firewall based networks, as well as future networks such as zero trust), we recommend the second sentence be removed. The second sentence, "These configurations or policies group CIP Systems of the same impact rating and their associated PCAs", seems to be an arbitrary statement that does not build upon the security requirement. A semantic argument could be made that once the configurations or policies are established, all CIP Systems inherit the highest water mark; however, prior to the establishment, the inherent risk of the associated CIP Systems could differ. We suggest removing the second sentence to avoid future confusive discussion.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
We suggest adding “routable protocol” to the revised definition. We feel this can still be used for both types of networks. We also suggest removing “CIP Systems,”and replace with “BES Cyber Systems.” Remove “enforced by an EACMS.”	

Suggested definition - *A set of configurations or policies (**Remove: enforced by an EACMS)** that controls routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber Systems of the same impact rating and their associated PCA.*

Likes 0

Dislikes 0

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.

Likes 0

Dislikes 0

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

OKGE supports EEI's comments.

Likes 0

Dislikes 0

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

Although the revised definition allows for both traditional firewall-based networks as well as more modern protections, the definition remains incomplete. We would suggest altering the definition as follows: “**A logical boundary defined by** a set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System and that groups CIP Systems of the same **or lower** impact rating”

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer	No
Document Name	

Comment

MEAG Power adopts the Southern Commany comments.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

The proposed change ignores the concept of an isolated ESP network and instead requires an EACMS be deployed regardless to control communications between BCS, PCAs within the same network. The application of an EACMS in an isolated ESP network would add no extra protections or benefit for the purpose of controlling communications within the network given there are no Electronic Access Points applicable in relation to routable traffic from outside of the ESP or exiting the ESP.

BC Hydro recommends clarifying that the EACMS requirement portion of the definition be applicable only in cases where ERC may exist (i.e. discrete ESPs or extended ESPs).

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No
Document Name	

Comment

New ESP definition would disallow including assets of lower impact ratings in a higher security environment, thus preventing the potential implementation of security best practices on Medium or Low impact assets. The new definition of ESP would also prevent the use of VLANs as a method of demonstrating isolation of BCS and other Cyber Assets as the Switches involved with managing of VLANs are often classified as BCAs and under the current CIP standards an asset classified as a BCA cannot be classified also as an EACMS, PCA or PACS.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

The second sentence appears to be redundant due to the phrase “and their associated PCAs” since PCAs are included within the proposed “CIP System” definition. SIGE proposes the following:

“A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System and that groups CIP Systems of the same impact rating.”

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA supports most of the definition change, however "policies" are a vague reference. NCPA proposes using the phrase "technical policies" as to not confuse them with administrative policies.

Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	

The second sentence appears to be redundant due to the phrase "and their associated PCAs" since PCAs are included within the proposed "CIP System" definition. CEHE proposes the following:

"A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System and that groups CIP Systems of the same impact rating."

Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	

There is no clear point of demarcation where the border of the ESP is defined, introducing significant concerns how the boundary of the CIP standard will be evaluated and enforced. Recommend retaining current definition. While not necessary, it may be appropriate to clarify that additional controls may be implemented within the security perimeter to limit communication ports inside of requirement CIP-007 R1.1

Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	No

Document Name	

Comment

While we do not believe it to be the intent of the SDT, we disagree with the new definition(s) of EACMS and ESP as it is less clear what is and is not considered an ESP. Currently, a substation facility BCS that is not utilizing routable protocols, such as an RTU serially connected to several relays, is not classified as an ESP and subsequently, the RTU (which could be used as a central access point to the relays) would not be classified as an EACMS. This clarity is lost with the proposed definition changes.

Recommendation:

Electronic Security Perimeter (ESP) – The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or

A set of configurations or policies enforced by an EACMS that controls routable communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Electronic Access Control or Monitoring Systems (EACMS) – Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring via routable protocols of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Intermediate Systems and SCI grouped by the Responsible Entity, in the EACMS it supports.

Likes 0	
Dislikes 0	

Response

Ronald Bender - Nebraska Public Power District - 5

Answer	No
Document Name	

Comment

We agree that the proposed ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. However, the routable protocol qualifier was removed and the new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. This seems like a circular definition. Also, it is our understanding that the SDT does not intend to have requirements baked into definitions but with the proposed ESP definition, and changes to CIP-005, the definition is the only place EACMS are required. We propose the following changes:

ESP definition: A set of configurations or policies that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

New CIP-005-X R1 Part 1.X:

Applicable Systems

High Impact BES Cyber Systems and their associated PCA

Medium Impact BES Cyber Systems and their associated PCA

Requirements

1.X.1 - EACMSs must be implemented to enforce ESPs where communication leaves the ESP, or where SCI is used.

1.X.2 - EAPs must be identified for ESPs.

When the proposed ESP definition is applied in the proposed CIP-005-X R1 Part 1.1 there is another issue since the definition no longer has the routable protocol qualifier. See our response to Question #10 below for further explanation.

Likes 0	
Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5

Answer	No
Document Name	

Comment

See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

Duke Energy agrees with the directional change but has identified several concerns with the proposed language.

First, the use of CIP Systems in the definition is in conflict with the use of BES Cyber System as the initial scoping in the definition, as it could be interpreted to require ESPs around EACMS and PACS that are outside the traditional ESP boundary on separate hardware. Further, this introduces a redundancy between the CIP Systems and PCA definitions.

Second, the use of the term policies is ambiguous in context and is likely to be conflicted with written policies (e.g. procedurally requiring password rotation). Policy-based access control is configured into the enforcing system, and therefore is inherently included in the configuration term. This should be made explicit in measures or guidance documents to ensure the intent to allow future policy-based access control is apparent.

Third, the inclusion of qualifiers to address the host-based firewall concern in the requirement language is inappropriate as it addresses specific solutions. A better means of addressing this concern would be to include qualifiers in the definition of ESP to ensure that the configurations enforcing the perimeter do not reside on a BES Cyber Asset.

DUKE ENERGY PROPOSED DEFINITION FOR ESP:

A set of configurations enforced by an EACMS that creates a logical boundary where communications to or from any part of a BES Cyber System and any PCA or SCIG associated with a BES Cyber System are controlled. All BCS, PCA, and SCIG included in an ESP have the same impact rating as the highest included device. The EACMS enforcing the ESP may not be part of a BES Cyber System.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA agrees that the modified definition is more flexible for future ESPs using a zero trust environment. However, additional language is needed to address whether the SDT still intends for standalone networks that have no external connectivity to other networks (”standalone networks”) to have a defined ESP.

Option 1: If standalone networks DO NOT require an ESP, please update the Technical Rationale to address standalone networks (as was traditionally done in the TR for CIP-005-6 and CIP-005-7).

Option 2: If standalone networks DO still require an ESP, the proposed definition requires all ESPs to be “enforced by an EACMS;” this will add a high burden for standalone networks. For example, a standalone ESP consisting of a local operator HMI (PCA, used for local review of SCADA alarms) connected to 2 local SCADA RTUs (BCAs) via a switch (PCA) would need to have an EACMS added in order to meet the letter of the requirement, but without gaining any security or protection.

Option 2 proposed language: move the “enforced by an EACMS” from the definition of an ESP, to a new requirement for BCS with ERC:

(1) Definition for Electronic Security Perimeter (ESP): A set of configurations or policies that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Benefit: This would permit the isolated nature – or “configuration” – of the small local network to provide the control of communications to/from the BES Cyber System by simply excluding it.

(2) Add an additional requirement under CIP-005-8 R1.1 [hypothetically referenced here as R “1.1-A” for numbering clarity] for the EACMS portion:

Requirement: 1.1-A

Applicable Systems: BCS with ERC and their associated PCA Requirements: Utilize an EACMS to enforce the control of communications to or from any part of a BES Cyber System.

(3) Related update is needed to correct the Applicable Systems in R2.1: “EACMS that enforces an ESP for the Applicable Systems in Part 1.1-A.”

(4) Update the Technical Rationale (TR) to clarify for standalone networks (as was traditionally done in the **TR for CIP-005-6 and CIP-005-7**).

Likes 0	

Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
While the term ESP was restored, the definition shifted to a logical format much like ACLs while referencing the physical ESP with the definition of IRA Suggest clarify definition of ESP and IRA.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
The proposed change to the ESP definition adds a significant amount of ambiguity. Within the context of the new definition, the term “Electronic Security Perimeter” doesn’t seem to apply. ESP references a “perimeter” and the definition doesn’t indicate a logical perimeter of any sort. If anything, the definition essentially becomes synonymous only with the policies or rulesets mandated by a firewall. NRG recommends reverting the ESP term back to its original definition.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
The proposed change to the ESP definition adds a significant amount of ambiguity. Within the context of the new definition, the term “Electronic Security Perimeter” doesn’t seem to apply. ESP references a “perimeter” and the definition doesn’t indicate a logical perimeter of any sort. If anything,	

the definition essentially becomes synonymous only with the policies or rulesets mandated by a firewall. NRG recommends reverting the ESP term back to its original definition.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	Yes
Document Name	

Comment

The IRC SRC agrees that the proposed change to the ESP definition supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	Yes
Document Name	

Comment

We agree that the proposed change supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.”

The new definition can be used for both traditional firewall-based networks, as well as future networks such as zero-trust but we don’t agree on the overall definition.

The suggested definition broadens the current scope, it implies the presence of an EACMS, thus requesting another cyber asset (We have a BCA: VCA and we have an EACMS: Firewall) unless the SDT wanted to permit the double categorization (BCA/EACMS: a VCA with an embedded firewall)

The language “that controls communications” isn’t consistent with the NERC CIP orientation, usage of the bi-directional routable protocol should be used because with the current language one could imply that serial, layer 2 communication needs to have a set of configurations or policies.

Also, the definition states that this is for a BES Cyber System (…any part of a BES Cyber System…), yet the definition mention CIP System (… policies group CIP Systems of the same …). The definition of CIP System includes more than BES Cyber System.

We suggest reviewing the definition.

The proposal could be A set of configurations or policies enforced those controls bi-directional routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber System of the same impact rating and their associated PCAs. Reference: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	Yes
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT supports the IRC SRC comments.	
Likes 0	
Dislikes 0	
Response	
Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	Yes

Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	Yes
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
The new ESP may be logical/virtual or physical boundary applied using firewalls and zero trust.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	

We agree that the proposed ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	Yes
Document Name	

Comment

In support of IRC SRC/SWG.

We agree that the proposed change supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	Yes
Document Name	

Comment

Suggest the following modification to the ESP definition:

“These configurations or policies ***protect a*** group of CIP Systems of the same impact rating and their associated PCAs.”

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We agree that the proposed change supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.”

The new definition can be used for both traditional firewall-based networks, as well as future networks such as zero-trust but we don’t agree on the overall definition.

The suggested definition broadens the current scope, it implies the presence of an EACMS, thus requesting another cyber asset (We have a BCA: VCA and we have an EACMS: Firewall) unless the SDT wanted to permit the double categorization (BCA/EACMS: a VCA with an embedded firewall)

The language “that controls communications” isn’t consistent with the NERC CIP orientation, usage of the bi-directional routable protocol should be used because with the current language one could imply that serial, layer 2 communication needs to have a set of configurations or policies.

Also, the definition states that this is for a BES Cyber System (…any part of a BES Cyber System…), yet the definition mention CIP System (… policies group CIP Systems of the same …). The definition of CIP System includes more than BES Cyber System.

We suggest reviewing the definition.

The proposal could be

A set of configurations or policies enforced those controls bi-directional routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber System of the same impact rating and their associated PCAs.

Reference: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	Yes
Document Name	

Comment

In support of NPCC RSC comments.

We agree that the proposed change supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.”

The new definition can be used for both traditional firewall-based networks, as well as future networks such as zero-trust but we don’t agree on the overall definition.

The suggested definition broadens the current scope, it implies the presence of an EACMS, thus requesting another cyber asset (We have a BCA: VCA and we have an EACMS: Firewall) unless the SDT wanted to permit the double categorization (BCA/EACMS: a VCA with an embedded firewall)

The language “that controls communications” isn’t consistent with the NERC CIP orientation, usage of the bi-directional routable protocol should be used because with the current language one could imply that serial, layer 2 communication needs to have a set of configurations or policies.

Also, the definition states that this is for a BES Cyber System (…any part of a BES Cyber System…), yet the definition mention CIP System (… policies group CIP Systems of the same …). The definition of CIP System includes more than BES Cyber System.

We suggest reviewing the definition.

The proposal could be

A set of configurations or policies enforced those controls bi-directional routable protocol communications to or from any part of a BES Cyber System. These configurations or policies group BES Cyber System of the same impact rating and their associated PCAs.

Reference: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	Yes
Document Name	

Comment

We support NPCC TFIST's comments as found below:

We agree that the proposed change supports 1) traditional firewalls and 2) zero trust. However, the new language expands scope with “EACMS that controls communications to or from any part of a BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	Yes
Document Name	

Comment

SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that the modified ESP definition can be used for both traditional and future networks. However, the inclusion of the phrase “and their associated PCAs” is redundant and unnecessary since CIP Systems include associated PCAs by definition.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
The first sentence alone in the ESP definition seems to be able to be used for both traditional firewall-based networks and future networks. The second sentence is confusing in that a CIP System would have an associated PCA when PCA is already part of the CIP System definition.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Xcel Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Chelan agrees with the proposed definition changes for ESP.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE agrees with the proposed definition of ESP. The SDT could, however, consider revision it to the following for clarification: • A boundary of protection set by configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs Texas RE does note, however, that the proposed change to CIP-005 R1.1 explicitly states that host-based firewalls that only protect the host on which they reside are not a sufficient control to meet compliance with the requirement. Mass deployment of host-based firewalls is one method by which an organization can work toward implementing a zero-trust security model. The SDT may wish to consider this in the evaluation of its proposed ESP definition.	
Likes 0	
Dislikes 0	
Response	

5. The SDT modified the IRA definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
The new IRA definition could expand scope significantly. For instance, the second bullet within the proposed IRA definition – "through a Cyber Asset or Virtual Cyber Asset that is convering communications…" – could potentially bring into scope an operator at a Control Center increasing megawatts at a Medium without ERC plant and classify that scenario as IRA.	
Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
The new IRA definition could expand scope significantly. For instance, the second bullet within the proposed IRA definition – "through a Cyber Asset or Virtual Cyber Asset that is convering communications…" – could potentially bring into scope an operator at a Control Center increasing megawatts at a Medium without ERC plant and classify that scenario as IRA.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
There is insufficient clarity provided within the proposed terms to ensure consistent understanding and identification of applicable traffic.	
Likes 0	

Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Suggest removing ‘Responsible Entity’s’ as it should still be considered IRA if a user at one entity, outside an ESP, connected remotely to another entity's ESP. Additionally, consider changing ‘person’ to Cyber Asset. The use of a person in the context being ‘outside an Electronic Security Perimeter’ does not make sense. Suggest the following - User-initiated real-time access from a Cyber Asset outside of the Electronic Security Perimeters (ESP) using a routable protocol: Bullets one and two are in the singular tense, consider changing bullets three and four from plural tense to single tense as well. Bullet three to – ‘To a Management Interface of a Shared Cyber Infrastructure; or’ and bullet four to – ‘To a Management Interface of an Electronic Access Control or Monitoring System that enforces an ESP.’	

Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
The use of ‘within an ESP’ doesn’t work with the new ESP definition. Alternative proposal: Replace ‘from outside of the Responsible Entity’s Electronic Security Perimeters’ with ‘from a Cyber Asset that is not protected by an Entity’s Electronic Security Perimeters’, and replace ‘within an ESP’ and ‘within an Electronic Security Perimeter’ with ‘protected by an Electronic Security Perimeter’. Additionally, focusing on Mangement Interfaces rather than SCI itself could allow access to the SCI through an additional port that doesn’t meet the definition of a Management Interface.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
This definition introduces significant ambiguity and would rely excessively on non-enforcable Technical rationales and guidelines. As a result, it is subject to significant ambiguity. This ambiguity is further increased by the change in the definition of ESP that removes a clearly defined border of the ESP.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	

The second bullet point is not clear. Need for clarification

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

The definition of 'IRA' is unclear on the overall impact to the current infrastructure. Please further clarify as the second bullet "through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;" suggests that non-CIP devices will fall under the purview of this definition with the use of the NERC-defined term "Cyber System" being contained within the above language

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE does not agree with the proposed changes to the Interactive Remote Access definition because it seems to be unnecessarily confusing due to unneeded information within the definition.

The first bullet “to a Cyber System within an ESP” covers access to any Cyber System including its user interface ports. Therefore it is unnecessary to have the third and fourth bullet items. The third bullet specifies Management Interfaces of SCI, and similarly the fourth bullet specifies the Management Interfaces of the EACMS that enforces an ESP. However both SCI and EACMS are Cyber Systems which are covered by the first bullet.

The purpose of the fourth bullet is to capture remote access through a “serial to IP” device, and to achieve this the bullet item goes through a complex explanation on the conversion of routable to non-routable communications and Cyber Systems not in an ESP. The same thing can be accomplished by removing the phrase “using a routable protocol” from the first part of the definition. Then, to capture Cyber Systems not within an ESP, it seems that including “… Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) …” would more clearly capture this.

In addition, CEHE understands that a cabinet can be a PSP, and someone standing outside of the cabinet and physically connecting to a system within a cabinet is not IRA. This situation is not a remote connection therefore is not IRA and may need to be explained in the technical rationale.

IRA should not be prescribed to only “a routable protocol”. It should include all methods by which this is accomplished, even by a dial-up connection. However, CIP-005-8 requirement R2 specifically excludes Dial-up Connectivity. This is how the process should work. The definition states what IRA is, and the requirements specify exactly what applies.

Based upon those thoughts CEHE proposes the following:

“A user initiated real-time electronic access by a person from outside of a Responsible Entity’s Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) to a CIP System within the Responsible Entity’s ESP or PSP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System’s user interfaces.”

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)

Answer	No
Document Name	

Comment

Comments:

Clarification is needed around the Management Interfaces of a Shared Cyber Infrastructure (SCI). Is the intent to limit the definition of Management Interfaces that manage SCI and the other bulleted items in the definition, or is the intent to include all Management Interfaces?

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE does not agree with the proposed changes to the Interactive Remote Access definition because it seems to be unnecessarily confusing due to unneeded information within the definition.

The first bullet “to a Cyber System within an ESP” covers access to any Cyber System including its user interface ports. Therefore it is unnecessary to have the third and fourth bullet items. The third bullet specifies Management Interfaces of SCI, and similarly the fourth bullet specifies the Management Interfaces of the EACMS that enforces an ESP. However both SCI and EACMS are Cyber Systems which are covered by the first bullet.

The purpose of the fourth bullet is to capture remote access through a “serial to IP” device, and to achieve this the bullet item goes through a complex explanation on the conversion of routable to non-routable communications and Cyber Systems not in an ESP. The same thing can be accomplished by removing the phrase “using a routable protocol” from the first part of the definition. Then, to capture Cyber Systems not within an ESP, it seems that including “… Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) …” would more clearly capture this.

In addition, SIGE understands that a cabinet can be a PSP, and someone standing outside of the cabinet and physically connecting to a system within a cabinet is not IRA. This situation is not a remote connection therefore is not IRA and may need to be explained in the technical rationale.

IRA should not be prescribed to only “a routable protocol”. It should include all methods by which this is accomplished, even by a dial-up connection. However, CIP-005-8 requirement R2 specifically excludes Dial-up Connectivity. This is how the process should work. The definition states what IRA is, and the requirements specify exactly what applies.

Based upon those thoughts SIGE proposes the following:

“A user initiated real-time electronic access by a person from outside of a Responsible Entity’s Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) to a CIP System within the Responsible Entity’s ESP or PSP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System’s user interfaces.”

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No
Document Name	

Comment

The definition states that the communication is to a system within an ESP, but the last bullet states that IRA applies to Management Interfaces for EACMS that enforce an ESP. The problem with this is that the Management Interface does not necessarily reside within the ESP.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE is concerned with the use of the term “real-time” as it is a defined word in the NERC Glossary. This could introduce confusion. Texas RE recommends removing this term from the language.

Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	No
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We support NPCC TFIST's comments as found below: Request clarification of the second bullet because it does not apply to any NERC CIP applicable system. Suggest changing from “through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an	

Electronic Security Perimeter;" to "to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;".	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
As written and presented, there is a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication, but have not adequately enforced protections to ensure that the ports are not used by malicious actors regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to ensure validity of communications to Applicable Systems. In addition, approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization and approval of SCI terminology and other definitions associated with virtualization as a whole.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	

Comment

The definition needs clarification that system-to-system communications are not considered IRA. Add the following sentence back to the end of the definition as with the currently approved definition: “Interactive Remote Access does not include system-to-system process communications.”

Likes 0

Dislikes 0

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0

Dislikes 0

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

In support of NPCC RSC comments.

Request clarification of the second bullet because it does not apply to any NERC CIP applicable system. Suggest changing from “through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;” to “to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;”.

The new definition of ESP mentions an ESP is a …set of configurations or policies enforced by an EACMS… This definition doesn’t establish a boundary (logical border) so the language outside of the Responsible Entity’s Electronic Security Perimeters (ESP) or within an ESP doesn’t work.

The introduction of the converting functionality is interesting.

We suggest reviewing the definition of ESP/IRA/EAP.

Alternate proposal

User-initiated real-time access by a person outside of BES Cyber System, using a routable protocol:

• to a BES Cyber System;

• through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a BES Cyber System

• To Management Interfaces of a Shared Cyber Infrastructure; or

• To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP.

Reference

User-initiated real-time access by a person from outside of the Responsible Entity’s Electronic Security Perimeters (ESP). using a routable protocol:

• to a Cyber System within an ESP;

• through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;

• To Management Interfaces of a Shared Cyber Infrastructure; or

• To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP believes additional clarity is needed to the proposed definition of Interactive Remote Access (IRA) and provides the following revised introduction sentence for consideration.

"A user initiated electronic access by a person from outside of a Responsible Entity's Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP) using a routable protocol to a CIP System within the Responsible Entity's ESP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System's user interfaces. This includes access to:

- *Cyber Systems within an ESP;*
- *Through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter*;
- *To Management Interfaces of a Shared Cyber Infrastructure; or*
- *To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP"*

We suggest "real-time" be stricken from the definition as we believe there is no function that would allow "a person" to interact with a system in any frame of time other than "real-time". While we recognize the attempt to establish that this would not include batch processing, it is our opinion that the batch would run system-to-system and would not qualify as "a person".

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

We agree with the changes if real-time is being used as the NERC defined word. If that was the intent, it should be capitalized. If not, there should be more clarification around what real-time is. We agree if the intent is to continue to exclude system to system process communications.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Request clarification of the second bullet because it does not apply to any NERC CIP applicable system. Suggest changing from “through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;” to “to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;”.

The new definition of ESP mentions an ESP is a …set of configurations or policies enforced by an EACMS… This definition doesn’t establish a boundary (logical border) so the language outside of the Responsible Entity’s Electronic Security Perimeters (ESP) or within an ESP doesn’t work.

The introduction of the converting functionality is interesting.

We suggest reviewing the definition of ESP/IRA/EAP.

Alternate proposal

User-initiated real-time access by a person outside of BES Cyber System, using a routable protocol:

• to a BES Cyber System;

• through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a BES Cyber System

• To Management Interfaces of a Shared Cyber Infrastructure; or

• To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP.

Reference

User-initiated real-time access by a person from outside of the Responsible Entity’s Electronic Security Perimeters (ESP). using a routable protocol:

• to a Cyber System within an ESP;

• through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;

• To Management Interfaces of a Shared Cyber Infrastructure; or

• To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP.

Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We disagree with the proposed changes because much of the existing IRA definition is clear and effective. The SDT should only clarify whether the entire communication path needs to be routable from the remote client to the end device. **Recommendation:** We recommend making a minor change to the existing IRA to clarify the concept of a routable protocol converting to non-routable so that it can meet the goal of the SAR. (See our proposed changes to IRA and rationale in Q1	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0

Dislikes 0

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

Third bullet should read “To Management Interfaces of an Shared Cyber Infrastructure ***within*** *an ESP*; or” unless the SDT is trying to bring IRA restrictions to devices outside an ESP. In which case the applicability should be expanded further.

Likes 0

Dislikes 0

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

The definition needs clarification that system-to-system communications are not considered IRA. Add the following sentence back to the end of the definition as with the currently approved definition: “Interactive Remote Access does not include system-to-system process communications.”

Likes 0

Dislikes 0

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
In support of IRC SRC/SWG. Request clarification of the second bullet because it does not apply to any NERC CIP applicable system. Suggest changing from “through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;” to “to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;”.	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	No
Document Name	
Comment	
The definition needs clarification that system-to-system communications are not considered IRA. Add the following sentence back to the end of the definition as with the currently approved definition: “Interactive Remote Access does not include system-to-system process communications.”	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	

Comment

We are concerned with the implications of these changes in conjunction with the changes in definition to ESP, EACMS, and the addition of serial communication. To avoid confussin we believe this needs to be clarified within CIP-005 that CIP-005 IRA requirements do not apply to BCAs or PCAs controlling access only to themselves (such as host-based firewalls) when a traditional EACMS and Access Point (such as a site firewall) is being used.

Likes 0

Dislikes 0

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

We disagree with the proposed changes because much of the existing IRA definition is clear and effective. The SDT should only clarify whether the entire communication path needs to be routable from the remote client to the end device.

Recommendation: We recommend making a minor change to the existing IRA to clarify the concept of a routable protocol converting to non-routable so that it can meet the goal of the SAR. (See our proposed changes to IRA and rationale in Q1.

Likes 0

Dislikes 0

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- IRA with ERC has been confusing for Entities to understand when the conversion to serial devices appears to now be in scope if configurations may be impacted using serial thus requiring, for example password changes within 15 months.
    - Please provide more examples including transitioning BCA currently without ERC when it becomes BCA with ERC under the new proposed definitions and standards. How and where is the change applied and if it will be part of CIP-002?
- Does a Non-CIP System distribution Relay now become a PCA because it is connected to the Medium Impact Serial converter if it supports IRA?

Likes 0

Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern supports the changes concerning clarity for IP-serial conversions, but does not support the changes for Management Interfaces such as those on an “EACMS that enforces an ESP”. An Intermediate System is an EACMS that helps enforce an ESP which could open up a “Hall of Mirrors” scenario where an Intermediate System is required to access an Intermediate System. This hall of mirrors is stated in the Applicable Systems column of CIP-005 R2.1 (in the clean version of CIP-005 that was posted, which differs from the redline).	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT supports the IRC SRC comments and offers these additional comments: • Bullet 2: This appears to be backwards. It reads like you are sending communications outside the ESP. • Bullet 3: Please clarify if “To Management Interfaces of a Shared Cyber Infrastructure” is only related to the Cyber Assets within the ESP. • Bullet 4: Adding “To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforces an ESP” expands the scope of the existing definition by protecting more than just what resides inside the ESP.	
Likes 0	

Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Comments: EEI asks for additional clarity for the proposed definition of IRA. It is unclear why the definition includes “real-time” when the proposed definition specifically applies to access by a person. If “real-time” was inserted for a specific purpose, then the SDT should provide a clear explanation. Additionally, if “real-time” is needed, EEI recommends that the definition also include “IRA does not include system to system process communications or read-only access.”

“A user initiated real-time electronic access by a person from outside of a Responsible Entity’s Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) using a routable protocol to a CIP System within the Responsible Entity’s ESP or PSP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System’s user interfaces. This includes access to:

1. *Cyber Systems within an ESP;*
2. *Through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;*
3. *To Management Interfaces of a Shared Cyber Infrastructure; or*
4. *To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP”*
5. ***IRA does not include system to system process communications or read only access**.*

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
The definition needs clarification that system-to-system communications are not considered IRA. Add the following sentence back to the end of the definition as with the currently approved definition: "Interactive Remote Access does not include system-to-system process communications."	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	

Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	

Comment	

Request clarification of the second bullet because it does not apply to any NERC CIP applicable system. Suggest changing from “through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;” to “to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;”.

The new definition of ESP mentions an ESP is a …set of configurations or policies enforced by an EACMS… This definition doesn’t establish a boundary (logical border) so the language outside of the Responsible Entity’s Electronic Security Perimeters (ESP) or within an ESP doesn’t work.

The introduction of the converting functionality is interesting.

We suggest reviewing the definition of ESP/IRA/EAP.

Alternate proposal

User-initiated real-time access by a person outside of BES Cyber System, using a routable protocol:

• to a BES Cyber System;

• through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a BES Cyber System

• To Management Interfaces of a Shared Cyber Infrastructure; or

• To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP.

Reference

User-initiated real-time access by a person from outside of the Responsible Entity’s Electronic Security Perimeters (ESP). using a routable protocol:

• to a Cyber System within an ESP;

• through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;

• To Management Interfaces of a Shared Cyber Infrastructure; or

• To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforce an ESP.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	No
Document Name	

Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
N&ST believes the first sentence, "User-initiated real- time access by a person from outside of the Responsible Entity's Electronic Security Perimeters (ESP) using a routable protocol" fails to account for Responsible Entities that only have ESPs at some of their in-scope facilities or, in some instances (e.g., a TO with only serial Med Impact BCS) have no ESPs at all. Suggested change: "User-initiated real- time access by a person from outside of the Responsible Entity's Electronic Security Perimeters (ESPs) using a routable protocol, or "User-initiated real- time access by a person from outside of a Responsible Entity asset that contains only serially-connected BCS using a routable protocol… (etc.)"	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)	
Answer	No
Document Name	
Comment	
The IRS SRC recommends the SDT clarify the second bullet under the Interactive Remote Access (IRA) definition because it does not apply to any NERC CIP applicable system. Suggest changing the language from: "through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;" to: "to a Cyber System within an ESP, through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol from a Cyber System not within an Electronic Security Perimeter;".	
Likes 0	
Dislikes 0	

Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	

Answer	Yes
Document Name	

Comment

Chelan agrees with the proposed definition changes for IRA.

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	Yes
Document Name	

Comment

Duke Energy generally supports the SDT's direction, but suggests several changes to address various concerns:

Duke recommends that the second bullet be updated to read more clearly: "through a Cyber Asset or Virtual Cyber Asset that converts the communication from a routable protocol to a non-routable protocol that is passed on to a Cyber System not within an ESP." This also consistently applies abbreviations after the first instance of the term is spelled out.

Duke has concerns with the application of the IRA definition to the Management Interfaces of EACMS that enforce ESPs. This may result in reliability impacts when an EACMS Firewall management interface can only be accessed by an IS that is secured in a DMZ behind that firewall, and a failure of the firewall prevents access to the IS. We would suggest that the last bullet be removed from the definition. Proposed requirements in CIP-005 R1 Part 1.2 should provide adequate protection for these interfaces.

Finally, Duke Energy recommends that the SDT either explicitly refer to the defined term "Real-time" or use alternative language to avoid auditor interpretations as seen in the difference between "adverse impact" used in the BCA definition and the defined term "Adverse Reliability Impact".

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed change to the IRA definition.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Agree with the change to IRA definition.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

6. The SDT modified the Management Interface definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI for this question.	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)	
Answer	No
Document Name	
Comment	
The IRC SRC requests the SDT clarify the second bullet under the Management Interface definition; i.e. “Provide lights-out management capabilities; or,” by replacing vendor terminology with language from the prior Management Module definition; i.e. “an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.” Request clarification of the term “out-of-band.” What is the out-of-band risk? What is the requirement addressing?	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	

Request clarification of the second bullet – “Provide lights-out management capabilities; or.” Suggest using the old language instead of a vendor’s term. The old language was “an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.”

Request clarification of the term “out-of-band.” What is the out-of-band risk? What is the requirement addressing?

The definition seems to be too specific, i.e. direct reference to SCI, LOM, and ESP. Why not a more generic and simple definition like

A user interface, logical interface, or dedicated physical port that is used to control the processes of initializing, deploying, and configuring a cyber asset, excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Reference

A user interface, logical interface, or dedicated physical port that is used to:

•   Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or

•   Provide lights-out management capabilities; or

•   Configure an Electronic Security Perimeter; excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the IRC SRC.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

The revised definition does provide improvement over what was provided in the last draft, however, additional clarity to the intended meaning of Management Interface is still needed. This may be possible through additional enhancements to the definition or through additional explanation/defining what a Management Interface is through the Rationale. EEI offers the following revised definition:

"A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems."

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC understands the intent of the SDT and the rationale for Management Interface; however, the concepts of Management Plane and Operational Plane were clearer. While ATC appreciates the attempt to consolidate these terms and views Draft 2 as an improvement over Draft 1, 'interface' may be an overly broad term. The words 'user interface' are doing some heavy lifting and while the application interface and physical interface are performing the same "user interface" function, they really are very different things. There may be room for entities to misinterpret the current definition to their own peril.

- Is the overall purpose to protect from lateral movement, or to protect from unauthorized access to a management system?
- Is identity the primary perimeter?
    - Would it help if the SDT considered that concept when reassessing this definition and corresponding requirement language?
- The communication channel from which management is performed must be segregated from the channel with which operational functions are performed.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT supports the IRC SRC comments and offers this additional comment:

- Please clarify whether the Management Interface includes configuration of BCSs and PCAs within the ESP.

Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern disagrees with the addition of “Configure an Electronic Security Perimeter” to the Management Interface definition. With the definition of ESP being “a set of configurations or policies”, a Management Interface is something that configures a configuration that controls communications of any type at all. See Q14 for an example of the issues caused by this construct. Southern suggests that requirements be written that apply to BES Cyber Systems and separate requirements that set clear expectations around the use and administration of electronic access controls (and by extension PACS) and begin the process of moving away from an EACMS as a ‘device’ focus.	
Likes 0	
Dislikes 0	
Response	
Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	

ACES feels the inclusion of “Configure an Electronic Security Perimeter” does not cover what is intended and leaves a gap. We feel EACMS is a more inclusive term in place of ESP. Use of EACMS instead of ESP would then include Intermediate Systems, which pose a risk if Management Interfaces are not protected. This would then be consistent with the IRA definition.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

We agree with the Management Interface definition, but disagree with the language in the definition. In our view, the definition should focus on in CIP scope management interfaces. “Provide lights-out management capabilities” should be removed since this criterion cannot make a management interface to fall within CIP scope. Also, we suggest changing “configure ESP” to “configure EAP” and “configure EACMS” to address the zero-trust mode (See our comments in Q4). Also, the Management Interface definition only covers the Management Interface of a management system such as vCenter that configures and manage SCI while the Hypervisor Management Interface that initializes, deploys and configures VCAs is missing from the definition. Furthermore, the Management Interface should include managing non-ESP model based on our comments in Q4.

Recommendation: We propose the following changes to Management Interface definition and rationale in Q1.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

The term lights-out management capabilities is unclear. Additionally, in our opinion it should be specified that individual BCA or PCAs only controlling access to themselves (such as host-based firewalls) and their user interfaces do not classify as EACMs and Management Interfaces.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

In support of IRC SRC/SWG.

Request clarification of the second bullet – “Provide lights-out management capabilities; or.” Suggest using the old language instead of a vendor’s term. The old language was “an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.”

Request clarification of the term “out-of-band.” What is the out-of-band risk? What is the requirement addressing?

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

ISO-NE requests that a term other than "lights out" be used in the definition to avoid diffuclty with interpretation related to marketing language related to such products. Please re-cast the definition related to "lights out" management interfaces with respect to the character of the functions supported by the interface and the potential for risk to Cyber Asset support for reliability functions.

Likes 0	

Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

We agree with the Management Interface definition, but disagree with the language in the definition. In our view, the definition should focus on in CIP scope management interfaces. “Provide lights-out management capabilities” should be removed since this criterion cannot make a management interface to fall within CIP scope. Also, we suggest changing “configure ESP” to “configure EAP” and “configure EACMS” to address the zero-trust mode (See our comments in Q4). Also, the Management Interface definition only covers the Management Interface of a management system such as vCenter that configures and manage SCI while the Hypervisor Management Interface that initializes, deploys and configures VCAs is missing from the definition. Furthermore, the Management Interface should include managing non-ESP model based on our comments in Q4.

Recommendation: We propose the following changes to Management Interface definition and rationale in Q1.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Request clarification of the second bullet – “Provide lights-out management capabilities; or.” Suggest using the old language instead of a vendor’s term. The old language was “an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.”

Request clarification of the term “out-of-band.” What is the out-of-band risk? What is the requirement addressing?

The definition seems to be too specific, i.e. direct reference to SCI, LOM, and ESP. Why not a more generic and simple definition like

A user interface, logical interface, or dedicated physical port that is used to control the processes of initializing, deploying, and configuring a cyber asset, excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Reference

A user interface, logical interface, or dedicated physical port that is used to:

• Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or

• Provide lights-out management capabilities; or

• Configure an Electronic Security Perimeter; excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment	
AEP supports EEI comments and revised definition on “Management Interface”. In addition, please see response to Question #14 related to nesting acronyms within definitions. The revised definition for SDT’s consideration reads: *“A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems.”*	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
In support of NPCC RSC comments. Request clarification of the second bullet – “Provide lights-out management capabilities; or.” Suggest using the old language instead of a vendor’s term. The old language was “an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.” Request clarification of the term “out-of-band.” What is the out-of-band risk? What is the requirement addressing? The definition seems to be too specific, i.e. direct reference to SCI, LOM, and ESP. Why not a more generic and simple definition like	

A user interface, logical interface, or dedicated physical port that is used to control the processes of initializing, deploying, and configuring a cyber asset, excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Reference

A user interface, logical interface, or dedicated physical port that is used to:

• Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or

• Provide lights-out management capabilities; or

• Configure an Electronic Security Perimeter; excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.

Likes 0	
Dislikes 0	

Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We support NPCC TFIST's comments as found below: Request clarification of the second bullet – "Provide lights-out management capabilities; or." Suggest using the old language instead of a vendor's term. The old language was "an autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system." Request clarification of the term "out-of-band." What is the out-of-band risk? What is the requirement addressing?	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	No
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	

Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Additional clarity is required around the concept of "user interfaces" that are in scope per the new definition vs. the physical user interfaces that are indicated as being out of scope. This is a confusing and contradictory element of the definition. The definition is very broad and would include interface ports such as PS2 mouse/keyboard ports. It is not clear as to how practical considerations of such ports that have connected mice and keyboards for example would need to be protected per the CIP-005-8 proposed standard requirements to permit only needed and controlled communications to and from Management Interfaces and deny all other communications. Alternatively, as an example, it is not clear from a practical sense of how, per CIP-007-7, one would prevent the sharing of the CPU and memory of keyboard/mouse user interface ports. BC Hydro recommends changing the reference per the bullet "Provide lights-out management capabilities' within the definition of Management Interface to a more generic reference such as "out-of-band management capabilities" to meet the security intent instead of limiting to a particular type/brand.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	

Comment

SIGE does not agree with the new Management Interface definition, because it singles out a few Cyber Systems within the definition. The definition should define what a Management Interface is, and the standards/requirements will pinpoint which Cyber Systems should be applied.

SIGE proposes the following:

“A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems.”

Likes 0

Dislikes 0

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA support the modified definition, but suggest the language out-of-band instead of lights-out, since it a more general industry term and associated with a particular vendor.

Likes 0

Dislikes 0

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE does not agree with the new Management Interface definition, because it singles out a few Cyber Systems within the definition. The definition should define what a Management Interface is, and the standards/requirements will pinpoint which Cyber Systems should be applied.

CEHE proposes the following:

“A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems.”

Likes 0

Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Request clarification of the second bullet – “Provide lights-out management capabilities; or.”	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
ACES feels the inclusion of “Configure an Electronic Security Perimeter” does not cover what is intended and leaves a gap. We feel EACMS is a more inclusive term in place of ESP. Use of EACMS instead of ESP would then include Intermediate Systems, which pose a risk if Management Interfaces are not protected. This would then be consistent with the IRA definition. AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	

We support the general approach. However, the language is written using “or”. As a result, a management interface that supports any lights out system. In cases such as CIP-007 R1.3, this may be inappropriately interpreted to bring in unrelated items such as a UPS that support these devices.

Likes 0

Dislikes 0

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer No

Document Name

Comment

AZPS agrees with the proposed definition included in EEIs comments filed in this matter. AZPS requests additional information on what “Lights-Out capabilities”includes.

Proposed Definition: “*A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems.”*

Likes 0

Dislikes 0

Response

William Steiner - Midwest Reliability Organization - 10

Answer No

Document Name

Comment

The proposed definition leaves a great deal of ambiguity about the intent of the ‘user interface, logical interface, or dedicated physical port’. While in most cases, an entity would likely choose to go to the physical or logical (VLAN/sub-interface) port level, there are concerns about an approach where the entity may try to only protect the user interface, leaving other ports (TCP/UDP) on the same physical/logical port unprotected. It is unclear how vCenter would be treated – MRO would interpret it to be a ‘user interface’ included with SCI (per SCI definition, “including the software and Management Interfaces”).

In an all-in scenario, how do the protections apply to a Management Interface that is a different Cyber Asset (CA) from the SCI. For example, if vCenter is a different CA than the SCI its managing, how does the applicability of in CIP-005, CIP-007 and CIP-010 extend to that different CA running vCenter become SCI identified independently or a Cyber Asset?

The SCI definition includes Management Interfaces, if the Management Interface is a separate Cyber Asset how does the applicability extend to the separate Cyber Asset? For example, if a central firewall management system is outside of the ESP, how would this system be protected in the all-in scenario, or will it be required to be inside an ESP?

Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
The proposed changes appear to require significant modification to our current network architecture without clearly indicating how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy supports a consolidated definition for the various management components that require protection but suggests the use of “Management System” instead of “Management Interface” for parity with BCS, Cyber System, etc. as the preferred terminology for Applicable Systems. Additionally, Duke requests that the SDT provide thorough implementation guidance to assist in correctly classifying systems that provide management functions but	

are not associated specifically with SCI (e.g. SCOM) as this definition may introduce a confusing break in consistency of classification between SCI management (e.g. vCenter) and other management tools.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The previously proposed term “Management Systems” provided better clarity for identification of systems that support patching, configuration management, anti-malware signature updates, and other management functions. This clarity was lost with the newly proposed term. Specifically, the ‘and’ clause in “Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure;’ seems to imply only inclusion of systems used for initial provisioning (e.g., installing an operating system & configuring a network card) as opposed to systems that supporting ongoing health and maintenance activities for deployed systems.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	

The inclusion of “user interface” within the Management Interface definition will overly broaden the impact of the proposed definition. NRG recommends removing “user interface” from the definition.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

The inclusion of “user interface” within the Management Interface definition will overly broaden the impact of the proposed definition. NRG recommends removing “user interface” from the definition.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

There appears to be ambiguity around what is meant by logical interface. Does “user interface” refer to graphical user interface? If not, what is the difference between a “user interface” and the excluded “physical user interfaces…”?

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	Yes
Document Name	

Comment

No comments

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	Yes
Document Name	

Comment

Defining the Management Interface is good however documenting in the CIP-002 when used as part of the SCI should be clarified.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	Yes
Document Name	

Comment

Agree with the modified Management Interface definition.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	Yes
Document Name	

Comment

No comment.

Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
The proposed changes are an improvement to the previous Management Module and Management Systems definition; however additional clarity could be provided when referring to "lights-out" management capabilites. All entities may not agree on the intent of the referenced term, it should be defined to address the ability for a system administrator to monitor and manage servers by remote control.	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
iLO is a branded technology for Hewlett-Packard. BPA suggests replacing “lights-out” terminology with “dedicated out-of-band”.	
Likes 0	

Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	Yes
Document Name	

Comment

With the improvements to scoping in Draft 2, Chelan agrees with the definition Management Interface.

Likes 0	
Dislikes 0	

Response

Dan Zollner - Portland General Electric Co. - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends clarifying the definition of Management Interface. It is unclear what the three terms user interface", "dedicated physical port", and "physical user interfaces mean. Texas RE recommends the following definition:	

Management Interface: Any interface that is used to provide interactive electronic access and:

• Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or

• Provide lights-out management capabilities; or

• Configure an Electronic Security Perimeter

Likes 0	
Dislikes 0	

Response

7. As discussed in the CIP Definitions and Exemptions Technical Rationale (TR), the SDT believes that the use of configurations or policy in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
NRG believes that the modified ESP definition reduces the burden of documenting ESPs in a zero trust environment. However, the modified ESP definition over complicates the documentation of ESPs in a traditional, firewall-based environment.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
NRG believes that the modified ESP definition reduces the burden of documenting ESPs in a zero trust environment. However, the modified ESP definition over complicates the documentation of ESPs in a traditional, firewall-based environment.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
There is insufficient clarity provided within the proposed terms to ensure that consistent understanding of the construct of policy – e.g.: whether policy refers to technical control or procedural document.	
Likes 0	

Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA agrees that this will reduce the burden of documenting ESPs in a zero trust environment. However, additional language is needed to address whether the drafting committee still intends for standalone networks that have no external connectivity to other networks (”standalone networks”) to have a defined ESP.

Option 1: If standalone networks DO NOT require an ESP, please update the Technical Rationale to address standalone networks (as was traditionally done in the **TR for CIP-005-6 and CIP-005-7**).

Option 2: If standalone networks DO still require an ESP, the proposed definition requires all ESPs to be “enforced by an EACMS;” this will add a high burden for standalone networks. For example, a standalone ESP consisting of a local operator HMI (PCA, used for local review of SCADA alarms) connected to 2 local SCADA RTUs (BCAs) via a switch (PCA) would need to have an EACMS added in order to meet the letter of the requirement, but without gaining any security or protection.

(1) Definition for Electronic Security Perimeter (ESP): A set of configurations or policies that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Benefit: This would permit the isolated nature – or “configuration” – of the small local network to provide the control of communications to/from the BES Cyber System by simply excluding it.

(2) Add an additional requirement under CIP-005-8 R1.1 [hypothetically referenced here as R “1.1-A” for numbering clarity] for the EACMS portion:

Requirement: 1.1-A

Applicable Systems: BCS with ERC and their associated PCA

Requirements: Utilize an EACMS to enforce the control of communications to or from any part of a BES Cyber System.

(3) Related update is needed to correct the Applicable Systems in R2.1: "EACMS that enforces an ESP for the Applicable Systems in Part 1.1-A."

(4) Update the Technical Rationale (TR) to clarify for standalone networks (as was traditionally done in the TR for CIP-005-6 and CIP-005-7).

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

Although Duke Energy disagrees with the inclusion of "policy" in the definition, the spirit of this modified definition provides explicit clarity that evolving security technologies can be used in compliance with the NERC CIP Standards and will assist Registered Entities and the ERO in documenting CIP-005 compliance with increasingly secure postures.

Likes 0	
Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5

Answer	No
Document Name	

Comment

See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Josh Johnson - Lincoln Electric System - 1

Answer	No
Document Name	

Comment	
We disagree based on the reasoning and alternative proposal outlined in question 4.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS doesn’t understand how the use of “configurations or policy” in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	No
Document Name	
Comment	
While Zero Trust and it’s assumption of assuming no network edge is an excellent security approach, it is necessary to ensure that a discrete boundary defines the edge of the auditable network. The current definitions significantly blur this border introducing uncertainty into what will be audited under the CIP standards and introduces opportunity for significantly different viewpoints between auditors and entities regarding the boundary of what will be subject to NERC compliance standards. We support adopting definitions and standards that support virtualization. However until this is resolved, it will be impossible to support the revised standards. We recommending basing the new definition around the previous definition of an ESP as it has a defined border.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No

Document Name	
Comment	
ACES feels no matter how zero trust environments are implemented, the policy (ies) or configurations will be highly complex and exponentially more difficult to prove strict compliance, thus increasing compliance burden. Additionally on the latest webinar, it was discussed each policy enforcement point would be an EACMS. In a Cisco based SDN, each switch port, switch port group, VLAN, or switch has an enforcement policy applied to it from the policy server, increasing the number of EACMS significantly, therefore increasing compliance burden. Another issue will be varying technology compared to firewall rules/ACL as used today. This will make auditing extremely complex and require an auditor to have significant knowledge of varying SDN/zero trust products to be able to accurately audit. AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	No
Document Name	
Comment	
We are not sure it reduces the burden as entities will have to prove to auditors they are compliant and we don't know at this point what audit evidence requests will look like. We also wish to verify that knowledge of the TR is not necessary for understanding or complying with the proposed revisions to CIP-005-X R1.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA supports most of the definition change, however "policies" are a vague reference. NCPA proposes using the phrase "technical policies" as to not confuse them with administrative policies.	

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
While it may be the SDT's intent to reduce ESP documentation burden for entities employing Zero Trust environments, the language of the standards themselves do not reduce any such documentation burden pertaining to ESPs. In fact, the requirements still require ESPs to be implemented. BC Hydro recommends adding clarifying language around documentation expectations when Zero Trust environments are implemented vs. traditional firewall bounded ESPs.	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	No
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	No
Document Name	
Comment	

MEAG Power adopts the Southern Company comments.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

We support NPCC TFIST's comments as found below:

We agree with the modified ESP definition. We do not agree this change reduces the documentation burden of ESPs in a zero-trust environment.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

OKGE supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

In support of NPCC RSC comments.

We agree with the modified ESP definition. We do not agree this change reduces the documentation burden of ESPs in a zero-trust environment.

Looking solely at the definition of ESP, the old definition required to simply produce a list of assets in a boundary, this resulted in a large ESP. Establishing these ESP was easy and there were only one criteria to evaluate (connected using a routable protocol), overall (less burden). The suggested definition permits potentially smaller ESP, so more ESP, but those ESPs come with more controls, i.e., configurations or policies enforced and EACMS. With the new definition, the burden of the demonstration is more.

The ideas behind the new definition are interesting and they could facilitate the instauration of a zero-trust environment, but those ideas don’t lessen the burden of compliance demonstrations.

Reference:

Old Definition: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol. Suggested Definition: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP agrees with EEI's concern that it is unclear how the use of the terms "configuration or policy" reduces the burden of documenting ESPs in a zero trust environment. AEP also supports EEI's recombination on providing additional clarity and examples. In addition, AEP suggests the removal of the second sentence in the proposed ESP definition as noted in response to Question #4 above.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

We agree with the modified ESP definition. We do not agree this change reduces the documentation burden of ESPs in a zero-trust environment.

Looking solely at the definition of ESP, the old definition required to simply produce a list of assets in a boundary, this resulted in a large ESP. Establishing these ESP was easy and there were only one criteria to evaluate (connected using a routable protocol), overall (less burden). The suggested definition permits potentially smaller ESP, so more ESP, but those ESPs come with more controls, i.e., configurations or policies enforced and EACMS. With the new definition, the burden of the demonstration is more.

The ideas behind the new definition are interesting and they could facilitate the instauration of a zero-trust environment, but those ideas don't lessen the burden of compliance demonstrations.

Reference:

Old Definition: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

Suggested Definition: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE has not seen how the modified ESP definition can reduce the burden of documenting ESPs in a zero-trust environment (see NSRF comments in Q4). Given that a zero-trust environment in virtualization layer is a non-ESP topology and ESP drawings are not needed, there is no compliance burden reduction. Resulting from our comments in Q4, the zero-trust model can be resolved by adding an alternative requirement in CIP-005 R1.1.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

In support of IRC SRC/SWG.

We agree with the modified ESP definition. We do not agree this change reduces the documentation burden of ESPs in a zero-trust environment.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Regardless of which direction we go in will always have a burden - and again each entity will still have to show the auditors we are compliant. Depending on the auditor and their intreption of the requirement - can become burdensome. We don’t understand the zero trust environment as defined.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We are concerned that in hybrid environments with traditional firewalls AND zero-trust or host-based firewall applications, the new definitions of ESP and EACMs could create a burden to industry by requiring additional protections (such as encryption and multifactor authentication) on communications between devices that are already protected inside an ESP by a traditional firewall, and actually discourages the use of multi-layered protection.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
We haven’t seen the modified ESP definition can reduce the burden of documenting ESPs in a zero-trust environment (see our comments in Q4). Given that a zero-trust environment in virtualization layer is a non-ESP topology and ESP drawings are not needed, there is no compliance burden reduction. Resulting from our comments in Q4, the zero-trust model can be resolved by adding an alternative requirement in CIP-005 R1.1.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	

Comment	
• The ESP definition enables virtualization and logical boundaries but is not really going to reduce the documentation load. Zero trust will require documentation of where controls are applied including locations. • The IP to serial conversion for ERC and IRA appears to require additional documentation beyond the ESP. Please clarify how Entities are expected to document the logical boundaries beyond the ESP for serial devices.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	

Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	
Eversource agrees with the modified ESP definition, however, Eversource does not agree this change reduces the documentation burden of ESPs in a zero-trust environment.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
ACES feels no matter how zero trust environments are implemented, the policy (ies) or configurations will be highly complex and exponentially more difficult to prove strict compliance, thus increasing compliance burden. Additionally on the latest webinar, it was discussed each policy enforcement point would be an EACMS. In a Cisco based SDN, each switch port, switch port group, VLAN, or switch has an enforcement policy applied to it from the policy server, increasing the number of EACMS significantly, therefore increasing compliance burden. Another issue will be varying technology compared to firewall rules/ACL as used today. This will make auditing extremely complex and require an auditor to have significant knowledge of varying SDN/zero trust products to be able to accurately audit.	
Likes 0	
Dislikes 0	
Response	
Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	

Answer	No
Document Name	

Comment

<duplicate>

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	No
Document Name	

Comment

AWS supports the implementation of zero-trust architectures in fulfilling the security objectives of the NERC CIP Standards, but is seeking clarity on the assertion that the use of configurations or policies in the modified ESP definition can reduce the burden of documenting ESPs in a zero-trust environment. In a zero-trust environment the ESPs implemented by a Responsible Entity become more granular increasing the compliance documentation needed to support each policy or set of policies applied.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern agrees with the focus on network access policies rather than strictly network subnets (while not disallowing it) as things progress towards zero trust. However, as more fully stated in Q4, the phrase “that control communications” is overly broad and the ESP definition has nothing that scopes it to network communications.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT supports the IRC SRC comments.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
It is unclear how the use of the terms "configuration or policy" reduces the overall burden of documenting ESPs in a zero-trust environment. Zero trust is not used under the current definition of ESPs within a substation environment and for those entities that plan to continue using traditional firewalls, their processes for maintaining documentation will remain unchanged. For this reason, EEI requests additional clarity and examples describing how the use of "configuration or policy" language in this definition reduces the current burdens of documenting ESPs.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

We agree with the modified ESP definition. We do not agree this change reduces the documentation burden of ESPs in a zero-trust environment.

Looking solely at the definition of ESP, the old definition required to simply produce a list of assets in a boundary, this resulted in a large ESP. Establishing these ESP was easy and there were only one criteria to evaluate (connected using a routable protocol), overall (less burden). The suggested definition permits potentially smaller ESP, so more ESP, but those ESPs come with more controls, i.e., configurations or policies enforced and EACMS. With the new definition, the burden of the demonstration is more.

The ideas behind the new definition are interesting and they could facilitate the instauration of a zero-trust environment, but those ideas don't lessen the burden of compliance demonstrations.

Reference:

Old Definition: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

Suggested Definition: A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

The IRC SRC agrees with the modified ESP definition; however, we disagree this change will reduce the burden of documenting ESPs in a zero-trust environment.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Chelan agrees with the change to ESP, but disagrees with the notion that the new definition reduces the burden of documenting ESPs in a zero trust environment, rather it simply enables zero trust to even be an option.	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
We agree with the modified ESP definition but are not sure it reduces the burden as entities will have to prove to auditors they are compliant and we don’t know at this point what audit evidence requests will look like. We would also like to point out that because the routable protocol qualifier was eliminated from the ESP definition, and changes to the CIP-005 R1 Part 1.1, serial connectivity in some cases has been brought into the scope of an ESP. Refer to question #10 below.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	

Answer	Yes
Document Name	
Comment	
Suggest removing ‘and their associated PCAs’ from the ESP definition as PCAs are already included in the CIP Systems definition. ‘These configurations or policies group CIP Systems of the same impact rating (and their associated PCAs) delete this.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE proposed an ESP definition in response to question #4. However, it maintained the SDT approach on the use of configurations or policy. This does seem to have the potential of reducing the burden of documenting ESPs in a zero-trust environment.	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE proposed an ESP definition in response to question #4. However, it maintained the SDT approach on the use of configurations or policy. This does seem to have the potential of reducing the burden of documenting ESPs in a zero-trust environment.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	

Answer	Yes
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Yes, although PNMR appreciates EEI suggestion regarding "...clarity and examples describing how the use of “configuration or policy” language in this definition reduces the current burdens of documenting ESPs."	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	

Comment	
We agree with the modified ESP definition but are not sure it reduces the burden as entities will have to prove to auditors they are compliant and we don't know at this point what audit evidence requests will look like. We would also like to point out that because the routable protocol qualifier was eliminated from the ESP definition, and changes to the CIP-005 R1 Part 1.1, serial connectivity in some cases has been brought into the scope of an ESP.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends registered entities continue documenting ESPs in order to demonstrate compliance and show evidence of configuration of a zero-trust environment.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power has no experience with zero trust environments and has no feedback.	
Likes 0	
Dislikes 0	
Response	

8. The SDT added new and revised several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

Dan Zollner - Portland General Electric Co. - 3

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question. Additionally, Portland General Electric Company has concerns regarding the Interactive Remote Access (IRA) defintion. In the second bullet of the definition, the clause "to a Cyber System not within an Electronic Security Perimeter" implies that IRA can exist in scenarios where a person has no intent of remotely connecting to a BES Cyber System or PCA. The proposed definition of a Cyber System includes any number of Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that may be either CIP or non-CIP. If an individual was remotely communicating through a protocol converter to a device like a PACS, EACMS, or non-CIP Cyber Asset existing outside the ESP, that would be considered IRA under the current definition even if those systems didn't have connectivity to a BES Cyber System. Portland General Electric Company believes changing the clause to "to a BES Cyber System not within an Electronic Security Perimeter" achieves the objective of controlling IRA to BES Cyber Assets that are serially connected to the BES Cyber System.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

The IRC SRC requests the SDT clarify ERC for serial – IP communications to ensure backwards compatibility. We understand the proposed definition will not be backwards compatible; e.g. CIP-005, R3.1 and CIP-007, R4.2. Is that correct?

In addition, we request the SDT clarify the definition for BES Cyber System Information (BCSI) to include “SCI identified independently, supporting an Applicable System.”

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST recommendations for the definitions of ERC, ESP, and IRA are in our responses to Questions 3, 4 and 5, respectively. N&ST respectfully suggests the following changes to these additional definitions:

> EAP: “A policy enforcement point or a Cyber Asset interface that controls routable communication to and from a BES Cyber System from outside its Electronic Security Perimeter.”

> IS: The statement within the current IS definition, “The Intermediate System must not be located inside the Electronic Security Perimeter,” should be retained.

> EACMS and PACS: N&ST recommends both definitions, which begin with “Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI),…” be modified to begin with, “Cyber Assets, Virtual Cyber Assets, Cyber Systems, or Shared Cyber Infrastructure (SCI),…” This would clarify that it’s permissible to group an SCI with the EACMS and/or the PACS it supports.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question. Additionally, Portland General Electric Company has concerns regarding the Interactive Remote Access (IRA) defintion. In the second bullet of the definition, the clause "to a Cyber System not within an

Electronic Security Perimeter" implies that IRA can exist in scenarios where a person has no intent of remotely connecting to a BES Cyber System or PCA. The proposed definition of a Cyber System includes any number of Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that may be either CIP or non-CIP. If an individual was remotely communicating through a protocol converter to a device like a PACS, EACMS, or non-CIP Cyber Asset existing outside the ESP, that would be considered IRA under the current definition even if those systems didn't have connectivity to a BES Cyber System. Portland General Electric Company believes changing the clause to "to a BES Cyber System not within an Electronic Security Perimeter" achieves the objective of controlling IRA to BES Cyber Assets that are serially connected to the BES Cyber System.	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	
Comment	

Request clarification on ERC for serial – IP communications. We understand this will not be backward compatible. Is that correct? Such as CIP-005 R3.1 and CIP-007 R4.2

Request clarification of the updated BCSI definition. We believe this new definition should include “SCI identified independently supporting an Applicable System.”

We suggest some additional work on the definitions (ESP/IRA/CIP System/SCI) and a better alignment with the current CIP language.

Also, some definition includes some requirements on CPU and memory (isolation/shared), those requirements are not future proof. Furthermore, the definitions by focusing on shared CPU and memory trend toward hypervisor-based virtualization and don’t seem to provide a clear framework around other types of virtualizations like containerization technology.

We Suggest that the SDT review the definitions, the need for defining new terms and the nested definitions.

Likes 0	
Dislikes 0	
Response	

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	
Comment	

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

see responses to previous questions

Some additional revisions:

Remove “TCA” from CIP Systems - A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, or Shared Cyber Infrastructure, or Protected Cyber Asset. [delete - or Transient Cyber Asset.]

Remove “or a PCA” from the Virtual Cyber Asset - A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure [delete - or a PCA.]

Add “protocol” to EAP - A policy enforcement point or a Cyber Asset interface that allows routable protocol communication to and from the BES Cyber System within an Electronic Security Perimeter.

Cyber Asset – consider not excluding SCI, keeping the original - Programmable electronic devices, including the hardware, software, and data in those devices; [delete - excluding Shared Cyber Infrastructure.]

Cyber System – we suggest reverting back to Cyber Assets where this is used or go with a generic “cyber system” term in the exemptions language. Leave cyber system an undefined term. Simplifying applicability can create increased scope in the requirements.

Shared Cyber Infrastructure – Please provide more information in the technical rationale on what is intended with “including the software.”

Management Interface – In the non-virtualized environments there are applications that manage the policy implementation of firewalls that would be both a Management Interface and an EACMS under the new requirements and definitions. Was this the SDT’s intent?

Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	

PJM signs on to the comments provided by the IRC SRC.

Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	
Regarding ERC, this is a substantial change to the definition of ERC that has a larger impact than in the context of addressing virtualized environments. Several of the terms have been removed from the proposed definitions but are still being used other definitions and standards. For example Management Systems and Management Module have been removed but are still used in the SCI definition and in the CIP-005 R2.1 Measures and through the CIP-005 violation severity levels.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Generally, EEI supports most of the new/revised terms, but we have concerns with the following terms:	

External Routable Connectivity (ERC): See our comments to Question 3 above.

Electronic Security Perimeter (ESP): See our comments to Questions 4 and 7 above.

Interactive Remote Access (IRA): See our comments to Question 5 above.

Management Interface: EEI disagrees with the practice of nesting other Glossary Terms within the definition of other Glossary Terms. This practice makes it difficult to support definition that might otherwise be supported. While there are a number of other examples of this practice (see SCI) Management Interface serves as a good example of our concern.

Protected Cyber Asset (PCA): EEI seeks additional clarifications on the qualifier of “excluding Virtual Cyber Assets that are being actively remediated prior to introduction to the ESP.” If the VCA, or physical Cyber Asset, is outside of the ESP, how could it be considered a PCA when the required attribute of a PCA is that it is inside an ESP? Please provide clarification.

Virtual Cyber Asset (VCA) – The current definition is unclear and possibly unnecessary given the intent is to simply provide an equivalent virtualized term for a Cyber Asset, which is not a system but a programmable electronic device. If the SDT believes this term is necessary, we suggest the following:

“A logical instance of a programmable device, including the software and data, hosted on Shared Cyber Infrastructure or a PCA.”

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

ATC continues to have some questions about ERC and devices wholly inside an ESP.

- Where does the chain end?
- Do Cyber Assets two hops removed from the IRA entry point inside the ESP, or the system to system routable communication path between a system inside and outside the ESP have ERC?

The use of the term asset may make it more difficult to determine where ERC exists. Non-CIP systems inside a Control Center “asset” that are connecting into a CIP System inside the same Control Center “asset” could be at varied trust levels and should be protected via ERC and IRA controls.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No

Document Name	
Comment	
ERCOT supports the IRC SRC comments and offers this additional comment: - SCI should not be excluded from the Cyber Asset definition. SCI meet the definition of Cyber Asset in that it is comprised of hardware, software, and data.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
LCRA is concerned with using CIP System incorrectly due to SDT intent to only use it as a “non-CIP System”. CIP System does not appear to be a necessary term. TCAs are included in the CIP System definition. However, CIP System is used in the definition of ESP. This is an example of the confusion associated with the term.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
For “CIP System”, Southern agrees with having defined terms as shorthand, such as in CIP-007 R1.3 with its use of “non-CIP Systems.” However, Southern disagrees with the inclusion and nesting of this broad term within *many other* definitions. Analyzing the resulting scope of nested definitions based on “CIP System” is problematic, and our answers to Q3 and Q4 are specific examples of issues in its inclusion in ERC and ESP definitions.	
Likes 0	
Dislikes 0	
Response	

Maggy Powell - Amazon Web Services - 7

Answer	No
Document Name	

Comment

In addition to the comments regarding the ESP definition provided in response to question 4, AWS offers comments on the terms: CIP System, Cyber System and Transient Cyber Asset.

The terms CIP System and Cyber System are similar and could easily be confused or misunderstood. Please clarify whether the term “System” implies that evidence of compliance can be presented at the system level rather than the device level.

In addition, we oppose and suggest reconsideration to the Transient Cyber Asset (TCA) definition revision that allows virtual machines running on a physical TCA to be treated as software on the device. As written, a Responsible Entity is not be required to apply the appropriate security controls to the virtual machines running on physical TCAs. For security purposes, Responsible Entities should be monitoring the state of the virtual machines running on their physical hardware for security issues. We propose removing the language “Virtual machines hosted on a physical TCA can be treated as software on that physical TCA” from the TCA definition, and modifying the VCA definition to read, “A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure, a PCA, or a TCA.”

Likes 0	
Dislikes 0	

Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE

Answer	No
Document Name	

Comment

<duplicate>

Likes 0	
Dislikes 0	

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

LCRA is concerned with using CIP System incorrectly due to SDT intent to only use it as a “non-CIP System”. CIP System does not appear to be a necessary term. TCAs are included in the CIP System definition. However, CIP System is used in the definition of ESP. This is an example of the confusion associated with the term.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- The ERC and IRA with serial conversion needs to be clarified with more industry use cases and may require improved language.
- External Routable Connectivity (ERC) language enhancement: The electronic bidirectional routable protocol communications between a CIP System and a Cyber System (Cyber Asset or Virtual Cyber Asset) located outside of the asset's PSP or ESP.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

We believe the definition of ERC is confusing because it is unclear what the term "asset" is referring to when it states "from outside the asset containing the CIP System". Is this referring to a cyber asset, a BES asset, or a Facility? The definition was much clearer when referring to an ESP. The additional concerns with definitions have been addressed above.

Likes 0	
Dislikes 0	

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	No
Document Name	

Comment	
Remove “TCA” from CIP Systems - A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, or Shared Cyber Infrastructure, or Protected Cyber Asset. [delete - or Transient Cyber Asset.] Remove “or a PCA” from the Virtual Cyber Asset - A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure [delete - or a PCA.] Add “protocol” to EAP - A policy enforcement point or a Cyber Asset interface that allows routable protocol communication to and from the BES Cyber System within an Electronic Security Perimeter. Cyber Asset – consider not excluding SCI, keeping the original - Programmable electronic devices, including the hardware, software, and data in those devices; [delete - excluding Shared Cyber Infrastructure.] Cyber System – we suggest reverting back to Cyber Assets where this is used or go with a generic “cyber system” term in the exemption's language. Leave cyber system an undefined term. Simplifying applicability can create increased scope in the requirements. Shared Cyber Infrastructure – Please provide more information in the technical rationale on what is intended with “including the software.”	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
In support of IRC SRC/SWG. Request clarification on ERC for serial – IP communications. We understand this will not be backward compatible. Is that correct? Such as CIP-005 R3.1 and CIP-007 R4.2 Request clarification of the updated BCSI definition. We believe this new definition should include “SCI identified independently supporting an Applicable System.”	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	

Comment

ISO-NE requests that a term other than "lights out" be used in the Management Interface definition to avoid difficlty with interpretation related to marketing language related to such products. Please re-cast the definition related to "lights out" management interfaces with respect to the character of the functions supported by the interface and the potential for risk to Cyber Asset support for reliability functions.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

See responses to previos questions.

Remove “TCA” from CIP Systems - A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, or Shared Cyber Infrastructure, or Protected Cyber Asset. **or Transient Cyber Asset**.

Remove “or a PCA” from the Virtual Cyber Asset - A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure **or a PCA**.

Add “protocol” to EAP - A policy enforcement point or a Cyber Asset interface that allows routable protocol communication to and from the BES Cyber System within an Electronic Security Perimeter.

Cyber Asset – consider not excluding SCI, keeping the original - Programmable electronic devices, including the hardware, software, and data in those devices; **excluding Shared Cyber Infrastructure**.

Cyber System – we suggest reverting back to Cyber Assets where this is used or go with a generic “cyber system” term in the exemptions language. Leave cyber system an undefined term. Simplifying applicability can create increased scope in the requirements.

Shared Cyber Infrastructure – Please provide more information in the technical rationale on what is intended with “including the software.”

Management Interface – In the non-virtualized environments there are applications that manage the policy implementation of firewalls that would be both a Management Interface and an EACMS under the new requirements and definitions. Was this the SDT’s intent?

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No

Document Name	
Comment	
See comments in Q#5 above. With regard to EEI's comment regarding definition of VCA PNMR disagrees that it needs to be altered to better conform with the Cyber Asset definition. SMEs within our company found the definition proposed by the SDT to be clearer and a better fit than the definition proposed by EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No

Document Name	

Comment

Request clarification on ERC for serial – IP communications. We understand this will not be backward compatible. Is that correct? Such as CIP-005 R3.1 and CIP-007 R4.2

Request clarification of the updated BCSI definition. We believe this new definition should include “SCI identified independently supporting an Applicable System.”

We suggest some additional work on the definitions (ESP/IRA/CIP System/SCI) and a better alignment with the current CIP language.

Also, some definition includes some requirements on CPU and memory (isolation/shared), those requirements are not future proof. Furthermore, the definitions by focusing on shared CPU and memory trend toward hypervisor-based virtualization and don’t seem to provide a clear framework around other types of virtualizations like containerization technology.

We Suggest that the SDT review the definitions, the need for defining new terms and the nested definitions.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

Minnesota Power has concerns about acronyms CSI and SCI being confused. The SDT needs to consider other terms as it is close to an existing one. The SDT should consider *Private Cloud Infrastructure (PCI)* or *Virtual Cloud Infrastructure (VCI)* which could help facilitate a move to Public Cloud Infrastructure should an entity decide to do so. The second term may provide more flexibility in utlizing public cloud resources where an entity decides public cloud is more effective.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

In general, AEP supports most of the new and revised terms, but we have concerns with the following terms:

- **BES Cyber System Information (BCSI)**: There is no need to call out SCI in the BCSI definition when it is already covered in BES Cyber System definition.
- **Cyber Assets**: While the exclusion of Shared Cyber Infrastructure (SCI) in Cyber Assets definition seems okay upfront, it gets very confusing when applying this definition along with other definitions, such as SCI and Virtual Cyber Asset (VCA). VCA definition says it might be hosted on SCI (i.e., “A logical instance of an operating system or firmware hosted on SCI or a PCA”); However, SCI definition says “SCI does not include the supported VCA or CA with which it shares its resources”. Implementation may become chaotic unless all four definitions of CA, VCA, SCI and PCA are all logically explained in a real life context.
- **External Routable Connectivity (ERC)**: See response to Question #3 above
- **Electronic Security Perimeter (ESP)**: See responses to Questions #4 and #7 above.
- **Interactive Remote Access (IRA)**: See response to Question #5 above.
- **Management Interface**: See response to Question #6 above.
- **Protected Cyber Asset (PCA)**: AEP seeks additional clarifications on the qualifier of “excluding VCA that are being actively remediated prior to introduction to the ESP.” If the VCA, or physical Cyber Asset, is outside of the ESP, how could it be considered a PCA when the required attribute of a PCA be that it is inside an ESP? Please provide clarification.
- **Shared Cyber Infrastructure (SCI)**: AEP in general supports the definition of SCI except for “identified independently” and the nested inclusion of the Management Interface term. Please see responses to Questions #2 and #6.
- **Transient Cyber Asset (TCA):** AEP seeks additional clarifications on the significance of "Virtual machines hosted on a physical TCA can be treated as software on that physical TCA". If there were stated outcome(s) of treating as software, it might be more clear (implications of treating as software, that is).

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

In support of NPCC RSC comments.

Request clarification on ERC for serial – IP communications. We understand this will not be backward compatible. Is that correct? Such as CIP-005 R3.1 and CIP-007 R4.2

Request clarification of the updated BCSI definition. We believe this new definition should include “SCI identified independently supporting an Applicable System.”

We suggest some additional work on the definitions (ESP/IRA/CIP System/SCI) and a better alignment with the current CIP language.

Also, some definition includes some requirements on CPU and memory (isolation/shared), those requirements are not future proof. Furthermore, the definitions by focusing on shared CPU and memory trend toward hypervisor-based virtualization and don’t seem to provide a clear framework around other types of virtualizations like containerization technology.

We Suggest that the SDT review the definitions, the need for defining new terms and the nested definitions.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	No
Document Name	

Comment

Some additional revisions:

Remove “TCA” from CIP Systems - A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, or Shared Cyber Infrastructure, or Protected Cyber Asset. **(Remove: or Transient Cyber Asset.)**

Remove “or a PCA” from the Virtual Cyber Asset - A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure **(Remove: or a PCA)**.

Add “protocol” to EAP - A policy enforcement point or a Cyber Asset interface that allows routable protocol communication to and from the BES Cyber System within an Electronic Security Perimeter.

Cyber Asset – consider not excluding SCI, keeping the original - Programmable electronic devices, including the hardware, software, and data in those devices **(Remove: ; excluding Shared Cyber Infrastructure).**

Cyber System – we suggest reverting back to Cyber Assets where this is used or go with a generic “cyber system” term in the exemptions language. Leave cyber system an undefined term. Simplifying applicability can create increased scope in the requirements.

Shared Cyber Infrastructure – Please provide more information in the technical rationale on what is intended with “including the software.”

Management Interface – In the non-virtualized environments there are applications that manage the policy implementation of firewalls that would be both a Management Interface and an EACMS under the new requirements and definitions. Was this the SDT’s intent?

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

OKGE supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

As stated in Question 3, we do not agree with the modification to the definition for ERC.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

We support NPCC TFIST's comments as found below:

Request clarification on ERC for serial – IP communications. We understand this will not be backward compatible. Is that correct? Such as CIP-005 R3.1 and CIP-007 R4.2

Request clarification of the updated BCSI definition. We believe this new definition should include “SCI identified independently supporting an Applicable System.”

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer	No
Document Name	

Comment

MEAG Power adopts the Southern Company comments.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI Comments

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No

Document Name

Comment

While the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the 'as is' state of the definitions associated with some of the proposed NERC Glossary terms per comments provided in this project comment/ballot submission.

Likes 0

Dislikes 0

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No
Document Name	

Comment

The CIP standards as currently written are sufficient to accommodate virtualization based on security objectives. The proposed changes to the standards are overly prescriptive and difficult to understand. The previous proposed revision of the standards by this Project also adequately expanded the potential use of virtualization without removing backwards compatibility. Such drastic changes will be difficult to comply with and pose a security risk to the grid as time is taken away from practicing security and applied towards implementing overly prescriptive compliance requirements that seem to be a hall of mirrors.

Likes 0

Dislikes 0

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE has listed below terms not previously covered by the questions above.

CIP System – Agree

Cyber Assets – Agree

Cyber System – Agree

EACMS – Agree.

EAP – Agree.

Intermediate Systems - Agree.

PACS – Agree

PCA – Agree

SCI – Agree

TCA – Agree

VCA – Since a VCA is a logical instance of a Cyber Asset it seems that the VCA definition should be like the Cyber Asset definition. The current proposed VCA definition is radically different than the Cyber Asset definition. For that reason, SIGE proposes:

“A logical instance of a programmable device, including the software and data, hosted on Shared Cyber Infrastructure or a PCA.”

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA supports the proposed changes to IRA and Management Interface, however all others we do not support, please see comments above.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE has listed below terms not previously covered by the questions above.

CIP System – Agree

Cyber Assets – Agree

Cyber System – Agree

EACMS – Agree.

EAP – Agree.

Intermediate Systems - Agree.

PACS – Agree

PCA – Agree

SCI – Agree

TCA – Agree

VCA – Since a VCA is a logical instance of a Cyber Asset it seems that the VCA definition should be like the Cyber Asset definition. The current proposed VCA definition is radically different than the Cyber Asset definition. For that reason, CEHE proposes:

“A logical instance of a programmable device, including the software and data, hosted on Shared Cyber Infrastructure or a PCA.”

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Several of the terms and their usage, especially SCI, lends ambiguity with their use in the Standards. Further clarifications and refinements of the terms should be given attention.

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	
Comment	

Individually each new or revised term is acceptable. On the whole, however, it makes for a somewhat confusing “alphabet soup” of acronyms which only those with past experience in these technologies are easily able to tell apart or know which term is the appropriate one to use for which compliance tasks. The multiple new terms confuse efforts to comply and thus entail, even if only minor, more compliance risk rather than less. Further, it is not clear why all these terms are needed if we have an acceptable definition for Virtual Cyber Asset and a revised definition of BES Cyber System that includes Virtual Cyber Assets. We recommend the SDT review the definitions again to determine if few terms are needed and, if a new term is needed, to provide further clarity on what it addresses that other definitions do not.

Likes 0	
Dislikes 0	
Response	

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	
Comment	

Need to define/clarify “asset” in the definition of ERC,

Need clarification for the IRA definition (second bullet point is not clear)

Need clarification for “identified independently” in the definition of SCI

“CIP System” Definition – Transient Cyber Asset (TCA) should not be seen as a part of any system. A TCA is an asset connected to a system for a limited period of time. If it has to be seen as a part of a system, it is no longer a TCA. Also, this term is, in some ways, redundant compared to BCS. Even if “CIP System” designates any group of assets under CIP requirements, TCA cannot be seen as a “system”. It is an asset.

“Cyber System” Definition – Very confusing regarding “CIP System” and “BCS” definitions. Need more precisions or details about the context and when those definitions are used.

Likes 0	
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	No
Document Name	
Comment	

We support adopting definitions and standards that support virtualization. However, it will be impossible to support the revised standards without a clearly defined demarcation of the auditable network infrastructure. We do not have a reasonable recommendation to meet this need using the current approach to the proposed CIP standards. The important items to consider are ensuring defined borders that clearly identify what is in and out of scope of the definitions, ensuring that a company that is implementing currently acceptable virtualization approach with high watermarking does not have extensive changes to their CIP programs, no inadvertent changes to compliance standards, and ensuring definitions that clearly separate hosts and guests within virtualization.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	No
Document Name	

Comment

AZPS does not agree with all changes to the NERC Glossary terms. AZPS agrees with the concerns included in EEIs comments filed in this matter regarding Cyber Assets and Virtual Cyber Assets.

Cyber Assets – This term should revert back to its original singular form. While the definition refers to programmable electronic devices, the term remains singular in form and intent. This change would also harmonize with the new definition for Virtual Cyber Asset, which is not pluralized.

Virtual Cyber Asset (VCA) – The current definition is unclear and possibly unnecessary given the intent is to simply provide an equivalent virtualized term for a Cyber Asset, which is not a system but a programmable electronic device. If the SDT believes this term is necessary, we suggest the following:

“A logical instance of a programmable device, including the software and data, hosted on Shared Cyber Infrastructure or a PCA.”

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

CIP System – The definition contains an implicit requirement for entities to identify CIP Cyber Systems. The definition should not leave it up to the entity to make this identification, it should be criteria-based to include all of the described types of CAs. Alternate proposal: *A BES Cyber System and* *all associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, Shared Cyber Infrastructure, Protected Assets, and Transient Cyber Assets.*

Transient Cyber Asset – The use of ‘network within an Electronic Security Perimeter’ no longer works with the new definition of ESP. Alternate proposal: replace ‘network within an Electronic Security Perimeter’ with ‘network protected by an Electronic Security Perimeter’. (Even though the ESP definition no longer includes ‘network’, it is reasonable that a network could be protected by an ESP protecting all BCAs on that network.)

Removeable Media - The use of ‘network within an Electronic Security Perimeter’ no longer works with the new definition of ESP. Alternate proposal: replace ‘network within an Electronic Security Perimeter’ with ‘network protected by an Electronic Security Perimeter’. (Even though the ESP definition no longer includes ‘network’, it is reasonable that a network could be protected by an ESP protecting all BCAs on that network.)

Likes 0	
Dislikes 0	

Response

Josh Johnson - Lincoln Electric System - 1

Answer	No
Document Name	

Comment

We disagree based on the reasoning and alternative proposal outlined in question 4.

Likes 0	
Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5

Answer	No
Document Name	

Comment

See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

Duke has a number of definition concerns that are enumerated in response to the specific questions where the definition is relevant. In addition to those concerns, Duke Energy believes the following definition changes are required for the successful implementation of 2016-02's goals:

CIP System – Duke Energy suggests removal of TCAs from this collection of other device types to ensure that there are no inadvertent changes to scoping that historically excluded TCA devices (e.g. list of Cyber Assets to be included on the ERT CA tab).

PACS/EACMS – definitions do not take advantage of the new Cyber System definition

Cyber System – Duke Energy suggests that the inclusion of the term group here may provide an auditor basis to expect REs to actively group things that otherwise would be passively addressed. Additionally, it would be helpful to clarify that Cyber Systems are not necessarily in CIP scope. Suggested language is as follows: One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure. Cyber Systems may or may not receive one or more NERC CIP classifications.

ESP – Duke notes that the proposed definition for ESP drops the term "boundary" which was helpful in ensuring that auditors correctly evaluated this term. We propose to add this concept back in a manner that supports future interpretation of how a boundary may be implemented. This helps to ensure that dependent definitions (e.g. PCA use of "within") remain compatible with this iteration of the standards. Duke's proposed definition is repeated from Question 4 here: "A set of configurations enforced by an EACMS that creates a logical boundary where communications to or from any part of a BES Cyber System and any PCA or SCIG associated with a BES Cyber System are controlled. All BCS, PCA, and SCIG included in an ESP have the same impact rating as the highest included device. The EACMS enforcing the ESP may not be part of a BES Cyber System."

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy supports the comments of EEI.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No

Document Name	
Comment	
The SDT should consider NIST based approaches focused on defined outcomes instead of being prescriptive based on existing technologies.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
As articulated in greater detail above in response to previous questions, NRG disagrees with several of the proposed changes to the NERC Glossary terms	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
As articulated in greater detail above in response to previous questions, NRG disagrees with several of the proposed changes to the NERC Glossary terms.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	No
Document Name	

Comment	
The definition of PCA is problematic. The first is the general issue with the CPU/memory affinity requirements. For details on this, see comments in Q14. The PCA definition has a specific problem however. It essentially places a requirement inside a definition. The implicit requirement is that a BES Cyber Asset cannot share CPU/memory with a non-BCS of the same impact rating or a Protected Cyber Asset.. This is similar to the problem the current standards have with the definition of IRA having a requirement in it. If the SDT wishes this to be an auditable requirement, they should place the requirement within the standards and not within the glossary of terms.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Please see the response in Q14.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
ACES agrees with the added and modified terms except where noted in the responses to the questions in this comment form.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	

Comment	
GSOC supports the majority of the revisions subject to its comment on particular definitions provided herein.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
We agree with the new definitions of VCA, SCI and Management Interface, but disagree with the language in the definitions. We disagree with the changes to the definitions of CA, ESP, ERC, EAP , IRA and CIP System. See our proposed changes to the new and existing definitions and rationale for the disagreement in Q1.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Agree with the new and revised definitions short of the SCI definition.	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 3	
Answer	Yes
Document Name	
Comment	

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

We agree with the new definitions of VCA, SCI and Management Interface, but disagree with the language in the definitions. We disagree with the changes to the definitions of CA, ESP, ERC, EAP , IRA and CIP System. See our proposed changes to the new and existing definitions and rationale for the disagreement in Q1.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	Yes
Document Name	

Comment

ACES agrees with the added and modified terms except where noted in the responses to the questions in this comment form.

AEPC signed on to ACES comments.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	Yes
Document Name	

Comment

Suggest removing 'by a Responsible Entity' from the following definitions as it is implied or already stated in parent requirements.

BCS - One or more BES Cyber Assets logically grouped to perform one or more reliability tasks for a functional entity, including Shared Cyber Infrastructure grouped in the BES Cyber System it supports.

CIP System - A Cyber System identified as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.

PACS - Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) (including SCI grouped in the Physical Access Control Systems it supports) that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Likes 0	
Dislikes 0	

Response

Ronald Bender - Nebraska Public Power District - 5

Answer	Yes
Document Name	

Comment

The definitions on their own are acceptable.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

AECI agrees with the new and revised several defined terms; however, the CIP standard are becoming increasingly difficult to understand and implement appropriately.

Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	

Response

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE recommends revising the definition of Shared Cyber Infrastructure (SCI) to indicate that SCI inherit the impact categorizations of all hosted VCAs. For example, the VCA definition states “A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure or a PCA.” Also, the BCA definition includes “…or Virtual Cyber Asset..” This could lead to interpretations that PCAs can host BCAs.

The proposed definition for Protected Cyber Asset is written in a way where Virtual Cyber Assets may be out of scope for security requirements despite being hosted on SCI that host critical systems, such as high impact BCS. These VCAs will hereafter be referred to as non-CIP VCAs. These non-CIP VCAs would not be required to be protected by an ESP pursuant to CIP-005 R1.1 and as such permitting any and all network traffic to them would be permissible. Additionally, as these non-CIP VCAs would not meet the definition of an applicable system in CIP-005 R1.1 then CIP-005 R1.3 would not apply and communications between the non-CIP VCAs and the SCI hosting them would be also permissible.

Texas RE notes that if there are security concerns related to network communications between CIP VCAs and their hosting SCI then these same concerns should be present for network communications between non-CIP VCAs and their hosting SCI. Texas RE proposes that the portion of the PCA definition “Share CPU or memory with any part of a BES Cyber System,” be revised to “Share CPU or memory with any part of a BES Cyber System or Shared Cyber Infrastructure,”

Texas RE seeks clarity around the description of the definition of Intermediate System in the Definitions and Exemptions technical rationale document. For the definition of Intermediate System, the “Definitions and Exemptions” technical rationale document states that requirement language has been removed from the definition. The specific example of where the Intermediate System must reside was provided, as the current definition of Intermediate System prevents Intermediate Systems from being located within ESPs. The technical rationale then goes on to say that such language has been moved to a mandatory requirement within CIP-005 R2. Texas RE believes this statement is a reference to CIP-005 R2.6.2.

Texas RE seeks clarity around this concept and proposes the following language for CIP-005 R2.6.3: Communications between Intermediate Systems and Applicable Systems of Part 2.1. must go through an EACMS enforcing an ESP.

Likes 0

Dislikes 0

Response

9. The SDT revised CIP-002 based on industry comments. Do you agree with the proposed changes to the CIP-002 Reliability Standard? If not, please provide the basis for your disagreement and an alternate proposal.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

A more detailed explanation of the rationale behind the addition addition of “discrete” needs to be provided for further clarification to enable an accurate response.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

No. Please see NRG’s response to question 2 for additional detail.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

No. Please see NRG’s response to question 2 for additional detail.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

CIP-002 should retain its focus on identification of BES Cyber Systems and the associated approval by the CIP Senior Manager.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy does not agree with proposed changes in CIP-002 and believe that the concept of SCI indenpednatly verified requires further clarity. We also support EEI comments on this question.

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

As further discussed in response to Questions 1 and 2, Duke Energy disagrees with the complexity added to the CIP-002 requirements. Based on our suggestion of the addition of an SCI Group defined term, simplified language proposed in response to Question 1 can be used.

In Requirement 1.3, the comma following BCS introduces confusion and should be removed to be clear that the SCI clause follows onto the identify clause, and is not a requirement for a separate/additional list of assets that contain SCI supporting low BCS. Alternatively, bulleting the requirement after “asset that contains:” may be clearer.

Changes to the Attachment 2 criteria 2.1 to incorporate the term “discrete” lose the context of the original RFI; if the SDT retains the new “discrete shared” language, a comma should be inserted between these terms, and clarification should be provided in the technical rationale to carry forward the clarification provided in the RFI. Additionally, the SCI bullet appears to exclude the possibility of independently identifying SCI at Generation facilities. If

this was the SDT’s intent, justification should be provided that explains why this option is not available to this facility type under section 2.1. Finally, Section 2.2 generally follows the same format as section 2.1 but was not given the second bullet related to SCI; was this intentional? If so, it would be helpful to provide explanation in an appropriate document.	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
While mostly in agreement, please see our comments above responding to question #1.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	

AZPS agrees with EEI’s comments around the concern that both data communication links and communication networks should be exempt. AZPS asks the SDT to explain why they are now excluding communications networks.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

The CIP-002 should maintain a section on BROS that establish the relationship with the BCS

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

The first draft contained the weighting to determine if a TOP Control Center met the medium impact criteria from CIP-002-6. The second draft reverted back to CIP-002-5.1a’s criteria 2.12’s language without informing the industry. While there is a new project to “study” the impacts to the BES with this change further delaying smaller entities compliance burden relief, it was not made clear to industry CIP-002’s language was being reverted back under this project and was not shown as a change/redline from the first or redlined in the second draft which is highly misleading. If it is possible to incorporate other projects modifying other CIP standards into this project, why not the approved CIP-002-6 and complete the study at a later time?

AEPC has signed on to ACES comments.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Several of the terms and their usage, especially SCI, lends ambiguity with their use in the Standards. Further clarifications and refinements of the terms should be given attention.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE does not agree with the proposed changes to the 4.2.3.2. Exemption because in the “Lessons Learned CIP Version 5 Transition Program CIP-002-5.1: Communications and Networking Cyber Assets” issued by NERC, “study participants [in the Implementation Study] made a distinction between devices facilitating network communication locally for the BES Cyber Systems and those facilitating network communication external to the BES Cyber System or Facility. Entities determined network devices used only for external communication were out of scope in association with the high or medium impact BES Cyber System.” The “Lessons Learned CIP Version 5 Transition Program CIP-002-5.1: Communications and Networking Cyber Assets” was authorized by the Standards Committee on October 29, 2015 and is “ERO Enterprise – Endorsed Implementation Guidance.” However, it is still not in the standards and auditors can only go by the standards and not “Lesson Learned” documents.

The “between discrete ESPs” exemption is too narrow; all Cyber Systems used only for external communication need to be exempt, not just those between discrete ESPs. The reason is that there are instances when the same Cyber Systems can be used between two discrete ESP and between an ESP and non-ESP site. In one instance the Cyber Systems are exempt, in the other they are not, even though it is the same equipment performing the same function.

This narrow exemption has the potential of pulling Cyber Systems used for only external network communications into scope. Entities may have to bring telecommunication sites into compliance, which could mean additional costs, physical and electronic controls that would otherwise not be needed, and possibly more staff to produce and maintain the documentation required for compliance. This could create a situation where an Entity may have to choose a leased network over a private network due to the leased network being exempt even though it performs the same function as a private system.

Private systems are usually more reliable than leased systems, so overall the BES would be less reliable when using a leased system which is directly opposite of the purpose of the NERC standards. Private systems should be encouraged and exempting all Cyber Systems used only for external communications would do that.

CEHE proposes the following:

“4.2.3.2. Cyber Systems used only for external network communication between assets, or one or more geographic locations.”

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA does not support the modified language in CIP-002. How SCI is to be independently identified is not clear.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE does not agree with the proposed changes to the 4.2.3.2. Exemption because in the “Lessons Learned CIP Version 5 Transition Program CIP-002-5.1: Communications and Networking Cyber Assets” issued by NERC, “study participants [in the Implementation Study] made a distinction between devices facilitating network communication locally for the BES Cyber Systems and those facilitating network communication external to the BES Cyber System or Facility. Entities determined network devices used only for external communication were out of scope in association with the high or medium impact BES Cyber System.” The “Lessons Learned CIP Version 5 Transition Program CIP-002-5.1: Communications and Networking Cyber Assets” was authorized by the Standards Committee on October 29, 2015 and is “ERO Enterprise – Endorsed Implementation Guidance.” However, it is still not in the standards and auditors can only go by the standards and not “Lesson Learned” documents.

The “between discrete ESPs” exemption is too narrow; all Cyber Systems used only for external communication need to be exempt, not just those between discrete ESPs. The reason is that there are instances when the same Cyber Systems can be used between two discrete ESP and between an ESP and non-ESP site. In one instance the Cyber Systems are exempt, in the other they are not, even though it is the same equipment performing the same function.

This narrow exemption has the potential of pulling Cyber Systems used for only external network communications into scope. Entities may have to bring telecommunication sites into compliance, which could mean additional costs, physical and electronic controls that would otherwise not be needed, and possibly more staff to produce and maintain the documentation required for compliance. This could create a situation where an Entity may have to choose a leased network over a private network due to the leased network being exempt even though it performs the same function as a private system.

Private systems are usually more reliable than leased systems, so overall the BES would be less reliable when using a leased system which is directly opposite of the purpose of the NERC standards. Private systems should be encouraged and exempting all Cyber Systems used only for external communications would do that.

SIGE proposes the following:

“4.2.3.2. Cyber Systems used only for external network communication between assets, or one or more geographic locations.”

Likes 0

Dislikes 0

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer No

Document Name

Comment

It is unclear what “independent SCI supporting any part of the high impact BCS…” is referring to.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer No

Document Name

Comment

As noted in the answer to Question #1, Texas RE recommends the language require identification of all BCS, as well as their associated EACMS, PACS, and PCAs. Absent that change, Texas RE recommends the SDT review Requirement R1 for logical flow. The proposed Requirement R1 language instructs registered entities to identify each BCS as either a BCS or as a BCS and independent SCI. Texas RE notes that it is not possible to identify a BCS as an independent SCI. If the system is a BCS then it must be identified as a BCS. The SDT could consider revising the language to:

1.1. Per Attachment 1, Section 1:

1.1.1. Identify each high impact BCS; and

1.1.2. Identify each independent SCI supporting any part of the high impact BCS or its associated EACMS, PACS, or PCAs.

1.2. Per Attachment 1, Section 2:

1.2.1. Identify each medium impact BCS; and;

1.2.2. Identify each independent SCI supporting any part of the medium impact BCS or its associated EACMS, PACS, or PCAs.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	No
Document Name	

Comment

SDG&E supports EEI Comments

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

We support NPCC TFIST's comments as found below:

Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain.

Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI?

Request correction of typo in R2 from the beginning “Each” to “The”

Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI?

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

OKGE supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
In support of NPCC RSC comments. Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain. Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI? Request correction of typo in R2 from the beginning “Each” to “The” Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI? The current wording creates more questions than answers. We suggest being more precise. See comments detailed in question one.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
"SCI independently identified" is frequently used throughout VSL in CIP-002, and "independent SCI" is used in the requirements. These phrases are not broadly understood and the intent needs to be clarified. In addition, AEP recommends SDT to add clarifying language to allow for the identification of both physical and virtual systems as EACMS, PACS and PCAs under CIP-002 as noted in response to Question #1.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
The concept of *independent SCI* needs to be defined as this leaves it wide open to interpretation for what it is and where it might exist. The SDT also needs to consider defining terms vBCA and vBCS, this may help to provide clarity to the industry.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	

Comment

We disagree with CIP-002 changes. CIP-002 R1 requirements should be restored and all other SCI language in CIP-002 Attachment 1 should be removed based on our comments in Q1.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain.

Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI?

Request correction of typo in R2 from the beginning “Each” to “The”

Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI?

The current wording creates more questions than answers. We suggest being more precise. See comments detailed in question one.

Likes 0	
Dislikes 0	

Response

Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5

Answer	No
Document Name	

Comment

Recommend including the definition within the text, or make a statement in the text directing to the definition in the definition list.

Likes 0	
Dislikes 0	

Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	No
Document Name	
Comment	
Remove the following phrases: from the second bullet on R1.1: “or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs)” and from the second bullet on R1.2: “or its associated EACMS, PACS or PCAs.” These are expanding the scope of the CIP-002 identification and CIP Senior Manager approval, and identification of these associated with SCI will create confusion since these do not have to be identified in CIP-002 if they are not associated with SCI. On Attachment 1, under the medium impact rating criteria 2.1, to clarify the second bullet, change it to begin: “Any SCI supporting BCS that could, within 15 minutes, adversely impact….” (Delete “(which must be included in a shared BCS),” “one or more” and “together.”	

Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE requests that the terms "high", "medium" and "low" used for impact ratings in the proposed CIP-002-7 be capitalized consistent with the rest of the CIP standards.	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 3	
Answer	No
Document Name	
Comment	
GRE agrees with the comments submitted by the NSRF.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
In support of IRC SRC/SWG. Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain	

Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI?

Request correction of typo in R2 from the beginning “Each” to “The”

Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI?

Likes 0

Dislikes 0

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	No
Document Name	

Comment

Remove the following phrases: from the second bullet on R1.1: “or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs)” and from the second bullet on R1.2: “or its associated EACMS, PACS or PCAs.” These are expanding the scope of the CIP-002 identification and CIP Senior Manager approval, and identification of these associated with SCI will create confusion since these do not have to be identified in CIP-002 if they are not associated with SCI.

On Attachment 1, under the medium impact rating criteria 2.1, to clarify the second bullet, change it to begin: “Any SCI supporting BCS that could, within 15 minutes, adversely impact….” **Delete** - “which must be included in a shared BCS,” “one or more,” and “together.”

Likes 0

Dislikes 0

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Please see our comments above responding to question #1.

Likes 0

Dislikes 0

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	No
Document Name	
Comment	
We disagree with CIP-002 changes. CIP-002 R1 requirements should be restored and all other SCI language in CIP-002 Attachment 1 should be removed based on our comments in Q1.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
• CIP-002 should include clarification for Cyber Assets with ERC that communications are converted serial needs to identify the risk to be mitigated applying the additional controls of ERC. ○ Entities are concerned many new CIP identified Cyber Asset using serial will come into scope requiring PSP controls and Password changes every 15 months.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
The first draft contained the weighting to determine if a TOP Control Center met the medium impact criteria from CIP-002-6. The second draft reverted back to CIP-002-5.1a's criteria 2.12's language without informing the industry. While there is a new project to "study" the impacts to the BES with this change further delaying smaller entities compliance burden relief, it was not made clear to industry CIP-002's language was being reverted back under this project and was not shown as a change/redline from the first or redlined in the second draft which is highly misleading. If it is possible to incorporate other projects modifying other CIP standards into this project, why not the approved CIP-002-6 and complete the study at a later time?	
Likes 0	
Dislikes 0	
Response	

Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1

Answer	No
Document Name	

Comment

Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain.

Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI?

Request correction of typo in R2 from the beginning “Each” to “The”

Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI?

Likes 0	
Dislikes 0	

Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE

Answer	No
Document Name	

Comment

<duplicate>

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	No
Document Name	

Comment

The modifications to CIP-002 are complex and include a number of new terms and concepts. For example, AWS supports the SDT’s addition of requirements for Management Interfaces, but Management Interfaces are not required to be identified in CIP-002. CIP-002 requires the identification of SCI and EACMS, not the associated Management Interface. This situation also occurs with Intermediate Systems under the currently enforceable

Standards and has been problematic. The embedded classifications increase the opportunity for compliance violations and security oversights. AWS suggests including those terms directly in CIP-002 for clarity. It would be helpful if the SDT provided in Implementation Guidance a logic diagram depicting how the device classifications and embedded definitions like Management Interface and CIP System can be applied. Lastly, the SDT has been clear that this project focuses on on-premise virtualization, however, many virtualization concepts could be interpreted as being related to cloud computing technologies. AWS suggests explicitly stating that the Standards do not apply to cloud within the Applicability section of CIP-002. If these updated Standards do not apply to cloud, it should be obvious to the reader.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT supports the IRC SRC comments and offers this additional comment: • Please see the ERCOT comments provided in Question 1.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI notes significant improvements to CIP-002 but asks for additional clarity for the following: 1) "SCI independently identified" is frequently used throughout CIP-002. This phrase is not broadly understood and the intent needs to be clarified. 2) In EEI's comments to the previous draft of CIP-002, we expressed concern regarding the proposed removal of communications networks from the Exemption Section of the previous draft, noting that both data communication links and communication networks should remain exempt. Nevertheless, this change remains in Draft 2 and EEI seeks clarification why communications networks remain excluded from the Exemptions section in this proposed draft of CIP-002.	

3) EEI recommends modifying 4.2.3.2 to align with endorsed ERO General Implementation Guidance titled “CIP Version 5 Transition Program, CIP-002-5-1: Communications and Networking Cyber Assets” dated October 6, 2015. EEI suggests the following: 4.2.3.2 Cyber Systems associated with: 4.2.3.2.1 Communication and networking devices between discrete Electronic Security Perimeters (ESP), and Cyber Systems associated with external communication to one or more geographic locations.” or 4.2.3.2.2 Non-routable communication externally directed between an ESP and one or more other geographic locations. or 4.2.3.2.3 Non-routable communication externally directed between BCS and one or more other geographic locations. 4) The inclusion of EACMS, PACS and PCAs seems redundant and possibly unnecessary in both the second bullet of R1.1 and the second bullet of R1.2. If this is an intentional, EEI request clarification within the Technical Rationale explaining the purpose of including of EACMS, PACS and PCAs.	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	
The requirement requires the identification of BCS as either “including any supporting SCI as part of the BCS” or with “independent SCI supporting any part of the high impact BCS or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).” This does not allow for the identification of BCS independent of having SCI, and therefore doesn’t account for non-virtualized environments. The requirements and measures of CIP-002 do not sufficiently detail what is required to demonstrate compliance. The requirements are to create a list that identifies “each [BCS] as either” including supporting SCI or having independent SCI. However, the independent SCI details an association to EACMS, PACS, PCA. The requirement expects an identification of “BES Cyber Systems” but the sub-bullets imply an expectation to identify SCI and corresponding asset/system classifications. The measures and technical rationale provide no additional clarity other than creating lists. Is the expectation to simply provide identification that the identified BCS either include SCI or are supported by SCI (e.g. Yes/No or Checkbox), or is the expectation to explicitly identify and categorize SCI that meet this criteria (e.g. “1.) ABC High Impact BCS; 2.) CDE High Impact EACMS SCI”). If the expectation is to classify SCI, what should be the approach for classifying SCI that supports multiple classifications (e.g. EACMS and PACS)? As mentioned in Comment for #2 above, more clarity regarding grouping SCI could be beneficial as well.	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No

Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Remove the following phrases: from the second bullet on R1.1: “or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs)” and from the second bullet on R1.2: “or its associated EACMS, PACS or PCAs.” These are expanding the scope of the CIP-002 identification and CIP Senior Manager approval, and identification of these associated with SCI will create confusion since these do not have to be identified in CIP-002 if they are not associated with SCI. On Attachment 1, under the medium impact rating criteria 2.1, to clarify the second bullet, change it to begin: “Any SCI supporting BCS that could, within 15 minutes, adversely impact….” (Delete “(which must be included in a shared BCS),” “one or more” and “together.”	
Likes 0	
Dislikes 0	
Response	

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification of capitalization of “High Impact,” “Medium Impact” and “Low Impact.” Parts 1.1, 1.2 and 1.3 use lower case while other Standards use capitalization. Is there a difference? If so, please explain.

Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCSI/SCI?

Request correction of typo in R2 from the beginning “Each” to “The”

Request clarification on the new (second) bullet in 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact asset could be consolidated into Medium Impact asset due to shared SCI?

The current wording creates more questions than answers. We suggest being more precise. See comments detailed in question one.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST believes the proposed revisions to Medium Impact Criterion 2.1 are confusing, particularly the parenthetical note in the second bullet that SCI “…must be included in a shared BCS” in order to potentially meet this criterion. If N&ST’s understanding of the SDT’s intentions regarding SCI, namely, that a Responsible Entity has the option of either including an SCI in a BCS (or an EACMS or a PACS) or identifying it as “independent” but supporting one or more BCS, EACMS, or PACS is correct, then we believe the second bullet, as written, is unnecessary. However, “independently identified” SCI that support BCS that meet Criterion 2.1 should be accounted for.

N&ST also believes the SDT should address the fact that Criteria 2.1 and 2.2, although ostensibly similar, are not consistent with each other: Criterion 2.2, as proposed, makes no mention of SCI at all.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

The IRC SRC requests the SDT clarify why the terms “High Impact,” “Medium Impact” and “Low Impact” are capitalized in some instances while in other instances; e.g. Parts 1.1, 1.2 and 1.3, lower case is used. Is there a difference? If so, please explain. If not, the IRC SRC recommends the SDT standardize the capitalization treatment of “High Impact,” “Medium Impact” and “Low Impact” throughout.

Request clarification on the “OR” in Part 1.3. What is the Entity required to identify? Assets or BCS/SCI?

Request correction of typo in R2 from the beginning “Each” to “The”

Request clarification on the new (second) bullet under 2.1 in Attachment 1. Does the SDT intend that a series of Low Impact assets could be consolidated into a Medium Impact asset due to shared SCI?

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	Yes
Document Name	
Comment	
Chelan approves of the revisions to CIP-002 but suggests clarification be made per comments for Q2.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
The draft CIP-002-7 standard now allows the Responsible Entity to identify SCI in the overall BCS or to identify them independently, it also requires the identification of SCI that supports EACMS, PACS, or PCAs. This gives Regional Entity enforcement staff the ability to identify noncompliance in a single requirement for a missed (SCI based) EACM, PACS, or PCA; rather than identifying all applicable requirements for a missed EACMS, PACS, or PCA.	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	

Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
We support these approach used for these changes once acceptable definitions are in place.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
However while the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the proposed changes to the NERC glossary of terms. BC Hydro does not agree with the 'as is' state of the SCI definition proposed in this project comment/ballot submission.	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
While mostly in agreement, we disagree with the SCI language and it should be removed from CIP-002.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC can support the changes to CIP-002 subject to ensuring the consistent identification of and reference to SCI.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
A long standing “error” appears to remain in the High VSL for R1, where it states “For Responsible Entities with a total of 100 or fewer high or medium impact and BCA, more than 10 but less than or equal to 15 identified BCA have not been categorized or have been incorrectly categorized at a lower category” where Medium and Severe mention “BCS” instead of “BCA” This is the only mention of BCA in the VSL. It appears as though the latest modifications only replaced definitions and did not correct this error.	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern generally agrees with the proposed changes to CIP-002 but with these suggestions for improvement. For R1.1 it would be clearer if it said “identify each high impact BCS as either of the following, if any, at each asset.” The same for R1.2, “identify each medium impact BCS as either of the following, if any, at each asset.” Both high and medium impact are clearly identified, and it does not imply that all BCS within an asset are of the same impact level. In addition, we suggest that CIP-002 not imply any process steps as identification methods vary within differing environments. Keep CIP-002 R1 as results-oriented as it has always been. We suggest capturing the options for SCI identification within the relevant definitions (as it currently is in the SCI proposal) and keep CIP-002 as close to the version 5.1a language as possible.	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Recommend spelling out “Shared Cyber Infrastructure” within CIP-002 standard text	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	

Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	

10. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

Dan Zollner - Portland General Electric Co. - 3

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question. Additionally, Replacing "BES Cyber System" with "CIP System" in the proposed definition of ERC appears to expand the scope of ERC from what was previously in place and now would include remote routable connectivity to PACS or EACMS. PGE wonders if this was the drafting team’s intent. If not, Portland General Electric Company believes the phrase "CIP System" in the proposed definition of ERC could be replaced with "BES Cyber System" to resolve the scope expansion.

Likes 0	
Dislikes 0	

Response

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question. Additionally, Replacing "BES Cyber System" with "CIP System" in the proposed definition of ERC appears to expand the scope of ERC from what was previously in place and now would include remote routable connectivity to PACS or EACMS. PGE wonders if this was the drafting team’s intent. If not, Portland General Electric Company believes the phrase "CIP System" in the proposed definition of ERC could be replaced with "BES Cyber System" to resolve the scope expansion.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces, and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request the SDT correct the typographical error, “Systerms” in Part 2.6.2 Requirements

Request the SDT clarify whether Exemption 4.2.3.3, which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations,” exempts any entity including third parties?

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST offers the following observations about the proposed changes to CIP-005:

> Regarding the statement in Requirement R1 Part 1.1 (“Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”), N&ST believes it is highly inappropriate to include such an explicit directive in a CIP Standard Requirement statement. Standard Drafting Teams have, in recent years, endeavored to make Requirements non-prescriptive. The should likewise be non-proscriptive. N&ST notes this proposed change seems to have been made in response to a concern about “logical isolation” that was expressed by a single individual, representing one organization, during the previous ballot’s comment period, which ended 3/22/2021. N&ST believes concerns about host-based firewalls may actually be moot, given the fact the SDT has dropped “logical isolation” and restored the better-defined “ESP.” However, if the SDT believes this prohibition should be put in writing, it should by all means be done, but in an implementation guide, not a Standard.

> N&ST believes Requirement R1 Part 1.2 (“Permit only needed and controlled communications to and from Management Interfaces,…”) should apply to SCI identified independently and to SCI that are grouped into BES Cyber Systems.

> N&ST believes Requirement R1 Parts 1.2 and 1.3 are largely redundant and should be combined.

> Regarding Requirement R2, Part 1.2, N&ST believes “Applicable Systems” should include EACMS inside an ESP, if any (there are such devices in practice today).

> N&ST recommends that the SDT “true up” the wording of Requirement R2 Part 2.5 and Requirement R3 Part 3.2, which both address disabling/terminating vendor remote connections, so that they both say the same thing.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5

Answer	No
Document Name	

Comment

Portland General Electric Company supports the comments provided by EEI for this survey question. Additionally, Replacing "BES Cyber System" with "CIP System" in the proposed definition of ERC appears to expand the scope of ERC from what was previously in place and now would include remote routable connectivity to PACS or EACMS. PGE wonders if this was the drafting team’s intent. If not, Portland General Electric Company believes the phrase "CIP System" in the proposed definition of ERC could be replaced with "BES Cyber System" to resolve the scope expansion.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request correction of the typo “Systerms” in Part 2.6.2’s Requirements

Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties?

Overall comment: We suggest reviewing the word ‘’communications’’, it should be a bi-directional routable protocol or a routable protocol. Communication is too vague. One could imply that serial, layer 2 communication needs to be controlled. If the intent of the SDT is to broaden the scope, why keep the notion of bi-directional routable protocol or routable protocol.

Requirement 1.1 New concept is inserted “between intelligent electronic devices”, what is an intelligent electronic device? We propose the SDT to use Cyber Asset definition.

The note regarding Host-based firewalls, is in sync with the definition of ESP, except we don’t agree on imposing this limitation. Also, the firewall wording is not used in the language of the requirements, controlled communication is the usual wording. We suggest the removal of this note.

The requirement should use the same language that is used for the other requirements. Suggestion

Applicable Systems connected to a network via a routable protocol must be protected by an ESP that Permits only needed and controlled communications and denies all other communications.

Requirement 1.2 We suggest reviewing the measure column. MPLS is mainly a WAN protocol. Also, a network switch enforces the VLAN concept so the network switch would be an SCI and EACMS? We suggest that the SDT review the mechanism permitting the control of communication. Someone could build a complete ecosystem with only a network switch (BCA is on VLAN 2 and the permitted users are on VLAN 2, the denied users are on VLAN 3, all of this is managed and controlled by a network switch, a switch this is virtualized.

Requirement 1.3 introductions of network communication. For some requirement, communication is the only word used (1.1, 1.2), we suggest that the SDT review the usage of the word ‘’network’’ and be uniform within all standards.

Requirement 1.4: No Comments

Requirement 1.5 version 6 of this requirement is only applicable to BCA and PCA, in this version the SDT as added PACS hosted on SCI; and EACMS hosted on SCI, and SCI identified independently supporting an Applicable System above. One could understand why the SCI is part of the applicable systems but why did the SDT target PACS and EACMS. We suggest to the SDT to remove PACS and EACMS. Also the line “SCI identified independently supporting an Applicable System above” should be replaced by the usual language used throughout the requirements, i.e.” SCI identified independently supporting an Applicable System from Part 1.1.” Clarification to that sentence would also be welcome, are they “SCI identified independently” or are they “SCI that is identified to be supporting independently an Applicable System”.

Requirement 1.6, this requirement is valid in the context of the old ESP definition. In the context of the suggested definition, this is an additional requirement resulting in a burden for the entity. The SDT should evaluate the possibility of enforcing the ESP controls (permitted communication and malicious communications) directly on the cyber asset itself, an EACMS wouldn’t be required. The BCA, PCA, EACMS, PACS, SCI could have their own controls (host firewall, host IDS, Host Endpoint controls).

Requirement 2.1 We suggest reviewing the Applicable column

EACMS that enforces an ESP for the Applicable Systems in Part 1.1.

This is an additional requirement resulting in an additional burden for the entity.

SCI identified independently supporting an Applicable System above

We suggest the normal wording (SCI identified independently supporting an Applicable System from Part 1.1.

Increase in the need for Intermediate System (EACMS used for the ESP, SCI).

Requirement 2.2 No Comments

Requirement 2.3 No Comments

Requirement 2.4 We suggest the SDT normalize the wording, ‘’from SCI identified independently supporting an Applicable System above’’ to ‘’SCI identified independently supporting an Applicable System from Part 1.1’’.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn’t have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.5 We suggest the SDT normalize the wording, ‘’from SCI identified independently supporting an Applicable System above’’ to ‘’SCI identified independently supporting an Applicable System from Part 1.1’’.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn’t have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.6. Requirement 2.6.1 is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization or consolidating services like databases or web applications. We suggest the SDT review their objectives and how to implement them. The reference to Part 2.1 in 2.6 can also be confusing for the requirement, does the restriction in CPU and memory also apply to the SCI in 2.1 or only to the Intermediate Systems.

Requirement 2.6.2 should use the same language that is used for the other requirements. Suggestion

Permit only needed and controlled communications and denies all other communications between Intermediate Systems and Applicable Systems of Part 2.1.

Reference 2.6.1, Restrict VCAs of Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI

Reference 2.6.2. Permit only needed and controlled communications between Intermediate Systems and Applicable Systems of Part 2.1.

Requirement 3 Is this a new requirement part of the SAR?

Also, requirement 2.4 and Requirement 2.5 doesn’t mention the ERC criteria for the Medium Impact BES Cyber Systems, yet requirements 3.1 and 3.2 mention the ERC criteria. This will increase the burden on the entities. We suggest the SDT review the scope and criteria.

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Remove Intermediate Systems from the applicability for 2.1 to permit authorized IRA through an Intermediate System (on the clean version).

R1.1 – The last sentence in the requirement is prescriptive and would be more appropriate in the technical rationale document. Consider removing this and moving it to TR: “Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”

R2.1 – Revise as follows to improve readability - Permit authorized IRA to Applicable Systems only through an Intermediate System.

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	No
Document Name	

Comment

PJM signs on to the comments provided by the IRC SRC.

Likes 0	
Dislikes 0	

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	
Agree with change to CIP-005. Do not agree with Glossary of Terms, especially new ERC Definitions in NERC Glossary of terms.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI generally agrees with many of the proposed NERC Glossary terms, but we also identified a number of proposed terms that remain a concern. EEI is specifically concerned with the phrase "SCI identified independently", which is not widely understood and needs to be clarified. For this and the following concerns we cannot support the proposed changes at this time. Requirement R1, subpart 1.4 may not fully cover the requirements set forth in CIP-006, Requirement R1, subpart 1.10. Associated PCAs are not included within subpart 1.4 but were specifically identified in CIP-006, subpart 1.10. This should be addressed or more clearly explained.	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	

ATC believes the SDT is close, however, we have concerns there could be unintended consequences with CIP-005 due to the changes to the ESP and IRA definitions as well as the newly proposed Management Interface definition. Additionally, please consider incorporating the routability aspect back into the ESP definition to clarify scope.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT supports the IRC SRC comments and offers these additional comments:.

- Please see the ERCOT comments provided in Questions 3 through 5 above.
- Please clarify the statement at the end about host-based firewalls in Part 1.1.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern disagrees with the applicability within R2. In R2.1, each Intermediate System is itself the object of the Intermediate System requirement, creating a hall of mirrors. Each Intermediate System is also an “EACMS that enforces an ESP”; it is an EACMS that enforces “policies or configuration” that “control communications”. See our fuller explanation of EACMS issues in Q14. In addition, there is an applicability difference between the clean and redline posted versions.

In addition, R2.6.2 points to the Applicable Systems of Part 2.1 as its applicability, however Part 2.1 includes the firewall (EACMS enforcing an ESP). We suggest R2.6.2 applicability should actually refer to Part 1.1, where only the BCS and the PCAs are in scope. That firewall (EACMS enforcing an ESP) is where one would implement R2.6.2, not the object of R2.6.2. Additionally, R2.6.2 has a spelling error (Systerms).

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	

The SDT is using the update to the definition as a mechanism to support zero-trust models, but the existing ESP definition does not preclude a Responsible Entity from applying the concept of zero-trust to its environment(s) in addition to its traditional ESP. The proposed modification does not obligate a Responsible Entity to adopt additional security controls.

The statement in the Definitions and Exemptions Technical Rationale, "[i]n these models, the perimeter shrinks to increasingly more granular levels, potentially down to a process or resource level on a BCS and nothing on the network is trusted for unrestricted communications," could be interpreted as meaning that traditional ESP-based perimeter security is not necessary or required. A Responsible Entity may choose to adopt a traditional ESP model, or a zero-trust model, without considering the benefits of a defense-in-depth approach that leverages both traditional perimeter-based security and zero-trust concepts.

AWS proposes the following language, "The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol that includes a set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs."

Detailed implementation guidance is necessary to support zero-trust and hybrid approaches.

AWS supports the implementation of zero-trust architectures in fulfilling the NERC CIP Standards, but is seeking clarity on the assertion that the use of configurations or policies in the modified ESP definition can reduce the burden of documenting ESPs in a zero-trust environment. As the ESPs implemented by a Responsible Entity become more granular in a zero-trust environment, the documentation needs to support each policy or set of policies applied seeming to increase the compliance documentation.

Likes 0	
Dislikes 0	
Response	

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	

<duplicate>

Likes 0	
Dislikes 0	
Response	

Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request correction of the typo “Systerms” in Part 2.6.2’s Requirements

Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties?

Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	No
Document Name	
Comment	

OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
• IRA and ERC when converted from routable IP to serial must be clarified. The language, application of and illustrations need to clearer. Additional and better use cases should be provided to address serial connected Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC generally agrees with the proposed revision to the term ESP, but is concerned that, despite those revisions, the term ESP is used inconsistently in CIP-005-8. As an example, the proposed language in CIP-005-8, R1.2 appears to have an inconsistency between the	

requirement and the measures. Specifically, the requirement language does not explicitly require an ESP while the measure appears to require an ESP. This also calls into question the inconsistent use of ESP between R1.1 and R1.2/1.3 and between these requirements and R1.6.

With the proposed modifications to the ESP definition, to avoid any confusion, it is recommended that specific language providing for traditional ESP protection of Applicable Systems be referenced as an option for meeting these requirements. Finally, if such language is not revised, GSOC requests clarification as to whether R1.6 is or should be applicable to any systems that are protected or are providing protections under R1.2 and R1.3 where those protections are not formally identified as an ESP. Inclusion of language such as “or other system or ESP” in Requirement R 1.6 would eliminate any uncertainty regarding protection of the Applicable Systems.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

We disagree with the changes in CIP-005.

Recommendations:

- For CIP-005 R1.1, we have provided recommendation in Q4.
- For CIP-005 R1.2 and R1.3, resulting from our proposed changes to the definition of SCI, BCA, EACMS, PACS and PCA, the devices containing Management Interface will be identified as BCA, EACMS, PACS or PCA, therefore CIP-005 R1.2 and R1.3 are no longer needed.
- For CIP-005 R1.4, we agree to moving the CIP-006 R1.10 to CIP-005 R1.4 that is the right spot.
- For CIP-005 R1.6, resulting from our proposed changes to the definitions, we suggest changing the Applicable Systems to the following:
- Electronic Access Points for High Impact BES Cyber Systems
- Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers
- EACMS that controls all communications to and from the BCS unless ESP model is used.
- For CIP-005 R2.1, it has a “hall of mirrors” issue since the Intermediate System requires another Intermediate System. Resulting from our proposed changes to the definitions, we suggest changing the Applicable Systems to the following:
- High Impact BES Cyber Systems and their associated PCA
- Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA
- EACMS that contains EAP

- EACMS that controls all communications to and from the BCS unless ESP model is used
- For CIP-005 R2.4 and R2.5, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.
- For CIP-005 R2.6, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA. We haven’t seen any problem for an Intermedium System to share resources with other types of CIP Cyber Assets.
- For CIP-005 R3.1 and R3.2, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

We also want to point out that CIP-005-8 R1 Part 1.1 specifically denies ‘*Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement*’ which does not meet the objective based model that the standards are supposed to now be written to. This very specifically identifies a technology that cannot be used to meet the requirement. This statement appears to be in conflict with the Technical Rationale for the ERC term.

ERC is no longer based on ‘external’ being defined in terms of the ESP as ESPs are changing in light of Zero Trust models. Zero Trust will shrink ESP’s over time to the smallest, most granular object possible including a single device or possibly to process or resource level on a device.

Question #10 begins by asking about the revised CIP-005 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-005.

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Please see comments regarding new definitions for ESP and EACMS. We believe the standard should address multi-layered access controls where traditional ESP boundaries are deployed using traditional firewalls, in addition to zero trust or host-based solutions. The IRA requirements should not apply to individual BCAs or PCAs with host-based solutions when they are also inside an ESP controlled by a traditional firewall.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No

Document Name	

Comment

NERC Definition Changes -- Electronic Security Perimeter (ESP) - removed the routable protocol qualifier. Consider the following:

* The new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. It seems like a circular definition.

When looking at the definitions only, it appears to require serial connected Cyber Assets have an EACMS to protect their serial communication links, however they are not required to have an Electronic Access Point (EAP) as the EAP definition has a routable communication qualifier.

When assessing CIP-005-8 R1.1 the Requirements section qualifies ESPs are only required for Applicable Systems with routable protocols. It does not have a qualifier of ERC so if there is only ethernet within a system that never leaves an asset, an ESP is required even if you have no EAP. This is the same as V5 of the standards.

If a BCA has both serial and Ethernet communications that leave an asset, auditors could require an EACMS for serial connections because a BCA that has routable protocol leaving an asset is required to have an ESP, and an ESP is required to have an EACMS. The same BCA serial that would leave the asset would require an EACMS because the ESP definition does not exclude serial communication. Not sure what type of device a serial EACMS would be.

The SDT proposed definition creates ambiguity around serial communication configurations and whether they have to be documented as part of an ESP.

We recommend revising CIP-005-X R1 Part 1.1 to read:

Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other commuincations. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement. Excluding:

* Time sensitive protection or control functions between intelligent electronic devices

* Cyber Asset to Cyber Asset serial communication not meeting the IRA definition

Additionally, question #10 begins by asking about the revised CIP-005 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-005.

Likes 0	
Dislikes 0	

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	No
Document Name	

Comment

Remove Intermediate Systems from the applicability for 2.1 to permit authorized IRA through an Intermediate System (on the clean version).

R1.1 – The last sentence in the requirement is prescriptive and would be more appropriate in the technical rationale document. Consider removing this and moving it to TR: “Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”

R2.1 – Revise as follows to improve readability - Permit authorized IRA to Applicable Systems only through an Intermediate System.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

In support of IRC SRC/SWG.

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces, and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request correction of the typo “Systerms” in Part 2.6.2’s Requirements

Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties?

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	

Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

Remove Intermediate Systems from the applicability for 2.1 to permit authorized IRA through an Intermediate System (on the clean version).

R1.1 – The last sentence in the requirement is prescriptive and would be more appropriate in the technical rationale document. Consider removing this and moving it to TR: “Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.”

R2.1 – Revise as follows to improve readability - Permit authorized IRA to Applicable Systems only through an Intermediate System.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

Regarding CIP-005 R1.3, PNM Resources disagrees with this requirement. The technical rational is to keep users on SCI from being able to manage the SCI.This can be done via CIP-005 R1.2 where only permitted communication is allowed. It may be possible that an entity has an administrator workstation that is also a BCA that can access both the data plane and management plane. CIP-005 R1.2 can restrict the network traffic to include the administrator workstation. In addition electronic access controls should be in-place on the Management Interface to only allow the appropriate administrators access to it. The prescriptive and broad ban of traffic from the data plan seems excessive. The separation occurs in cloud-based hosting because the hosting service is the administrator and the tenant is not. For on-premise that is not the case and the administrator and tenant are the same entity.

Does the SDT intend that those with on-premise virtualization purchase other physical workstation to manage the SCI? We cannot simply virtualize a PCA on the SCI to manage the SCI as it would be forbidden. The technical rational also is a bit inconsistent with the actual requirement. “The intent is users of a BCS hosted on an SCI that is identified independently and hosting other VCAs of differing impact levels should be prevented from having any access to the Management Interface of the underlying SCI.” The technical rational also doesn’t look at the 2nd and 3rd bullets in the definition of Management Interface, but only the first. The CIP-005 R1.3 requirement eliminates all BCS regardless of hosting status from having access to the Management Interface of the underlying SCI. We believe the controls in CIP-005 R1.2 along with electronic access controls for Management Interfaces is enough to prevent unauthorized users from managing the SCI or the EACMS that enforces the ESP. However CIP-005 R1.2 doesn’t address Management Interfaces on stand alone devices like physical server’s lights-out management port. If the SDT intends to fully protect lights-out management ports on stand-alone physical devices then it needs to be placed in scope in CIP-005 R1.2.

Regarding R2.1 missing a space in “Requirements” between “only” and “through”	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request correction of the typo “Systerms” in Part 2.6.2’s Requirements

Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties?

Overall comment: We suggest reviewing the word ‘’communications’’, it should be a bi-directional routable protocol or a routable protocol. Communication is too vague. One could imply that serial, layer 2 communication needs to be controlled. If the intent of the SDT is to broaden the scope, why keep the notion of bi-directional routable protocol or routable protocol.

Requirement 1.1 New concept is inserted “between intelligent electronic devices”, what is an intelligent electronic device? We propose the SDT to use Cyber Asset definition.

The note regarding Host-based firewalls, is in sync with the definition of ESP, except we don’t agree on imposing this limitation. Also, the firewall wording is not used in the language of the requirements, controlled communication is the usual wording. We suggest the removal of this note.

The requirement should use the same language that is used for the other requirements. Suggestion

Applicable Systems connected to a network via a routable protocol must be protected by an ESP that Permits only needed and controlled communications and denies all other communications.

Requirement 1.2 We suggest reviewing the measure column. MPLS is mainly a WAN protocol. Also, a network switch enforces the VLAN concept so the network switch would be an SCI and EACMS? We suggest that the SDT review the mechanism permitting the control of communication. Someone could build a complete ecosystem with only a network switch (BCA is on VLAN 2 and the permitted users are on VLAN 2, the denied users are on VLAN 3, all of this is managed and controlled by a network switch, a switch this is virtualized.

Requirement 1.3 introductions of network communication. For some requirement, communication is the only word used (1.1, 1.2), we suggest that the SDT review the usage of the word ‘’network’’ and be uniform within all standards.

Requirement 1.4: No Comments

Requirement 1.5 version 6 of this requirement is only applicable to BCA and PCA, in this version the SDT as added PACS hosted on SCI; and EACMS hosted on SCI, and SCI identified independently supporting an Applicable System above. One could understand why the SCI is part of the applicable systems but why did the SDT target PACS and EACMS. We suggest to the SDT to remove PACS and EACMS. Also the line “SCI identified independently supporting an Applicable System above” should be replaced by the usual language used throughout the requirements, i.e.” SCI identified independently supporting an Applicable System from Part 1.1.” Clarification to that sentence would also be welcome, are they “SCI identified independently” or are they “SCI that is identified to be supporting independently an Applicable System”.

Requirement 1.6, this requirement is valid in the context of the old ESP definition. In the context of the suggested definition, this is an additional requirement resulting in a burden for the entity. The SDT should evaluate the possibility of enforcing the ESP controls (permitted communication and malicious communications) directly on the cyber asset itself, an EACMS wouldn’t be required. The BCA, PCA, EACMS, PACS, SCI could have their own controls (host firewall, host IDS, Host Endpoint controls).

Requirement 2.1 We suggest reviewing the Applicable column

EACMS that enforces an ESP for the Applicable Systems in Part 1.1.

This is an additional requirement resulting in an additional burden for the entity.

SCI identified independently supporting an Applicable System above

We suggest the normal wording (SCI identified independently supporting an Applicable System from Part 1.1.

Increase in the need for Intermediate System (EACMS used for the ESP, SCI).

Requirement 2.2 No Comments

Requirement 2.3 No Comments

Requirement 2.4 We suggest the SDT normalize the wording, ‘’from SCI identified independently supporting an Applicable System above’’ to ‘’SCI identified independently supporting an Applicable System from Part 1.1’’.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn’t have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.5 We suggest the SDT normalize the wording, ‘’from SCI identified independently supporting an Applicable System above’’ to ‘’SCI identified independently supporting an Applicable System from Part 1.1’’.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn’t have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.6. Requirement 2.6.1 is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization or consolidating services like databases or web applications. We suggest the SDT review their objectives and how to implement them. The reference to Part 2.1 in 2.6 can also be confusing for the requirement, does the restriction in CPU and memory also apply to the SCI in 2.1 or only to the Intermediate Systems.

Requirement 2.6.2 should use the same language that is used for the other requirements. Suggestion

Permit only needed and controlled communications and denies all other communications between Intermediate Systems and Applicable Systems of Part 2.1.

Reference 2.6.1, Restrict VCAs of Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI

Reference 2.6.2. Permit only needed and controlled communications between Intermediate Systems and Applicable Systems of Part 2.1.

Requirement 3 Is this a new requirement part of the SAR?

Also, requirement 2.4 and Requirement 2.5 doesn’t mention the ERC criteria for the Medium Impact BES Cyber Systems, yet requirements 3.1 and 3.2 mention the ERC criteria. This will increase the burden on the entities. We suggest the SDT review the scope and criteria.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

We disagree with the changes in CIP-005.

Recommendations:

- For CIP-005 R1.1, we have provided recommendation in Q4.
- For CIP-005 R1.2 and R1.3, resulting from our proposed changes to the definition of SCI, BCA, EACMS, PACS and PCA, the devices containing Management Interface will be identified as BCA, EACMS, PACS or PCA, therefore CIP-005 R1.2 and R1.3 are no longer needed.
- For CIP-005 R1.4, we agree to moving the CIP-006 R1.10 to CIP-005 R1.4 that is the right spot.
- For CIP-005 R1.6, resulting from our proposed changes to the definitions, we suggest changing the Applicable Systems to the following:
    - Electronic Access Points for High Impact BES Cyber Systems
    - Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers
    - EACMS that controls all communications to and from the BCS unless ESP model is used.
- For CIP-005 R2.1, it has a “hall of mirrors” issue since the Intermediate System requires another Intermediate System. Resulting from our proposed changes to the definitions, we suggest changing the Applicable Systems to the following:
    - High Impact BES Cyber Systems and their associated PCA
    - Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA
    - EACMS that contains EAP
    - EACMS that controls all communications to and from the BCS unless ESP model is used
- For CIP-005 R2.4 and R2.5, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.
- For CIP-005 R2.6, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA. We haven’t seen any problem for an Intermedium System to share resources with other types of CIP Cyber Assets.
- For CIP-005 R3.1 and R3.2, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

NERC Definition Changes -- Electronic Security Perimeter (ESP) - removed the routable protocol qualifier. Consider the following:

- The new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. It seems like a circular definition.
- When looking at the definitions only, it appears to require serial connected Cyber Assets have an EACMS to protect their serial communication links, however they are not required to have an Electronic Access Point (EAP) as the EAP definition has a routable communication qualifier.

o When assessing CIP-005-8 R1.1 the Requirements section qualifies ESPs are only required for Applicable Systems with routable protocols. It does not have a qualifier of ERC so if there is only ethernet within a system that never leaves an asset, an ESP is required even if you have no EAP. This is the same as V5 of the standards.

o If a BCA has both serial and Ethernet communications that leave an asset, auditors could require an EACMS for serial connections because a BCA that has routable protocol leaving an asset is required to have an ESP, and an ESP is required to have an EACMS. The same BCA serial that would leave the asset would require an EACMS because the ESP definition does not exclude serial communication. Not sure what type of device a serial EACMS would be.

o The SDT proposed definition creates ambiguity around serial communication configurations and whether they have to be documented as part of an ESP.

We recommend revising CIP-005-X R1 Part 1.1 to read:

Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement. Excluding:

- Time sensitive protection or control functions between intelligent electronic devices
- Cyber Asset to Cyber Asset serial communication not meeting the IRA definition

We also want to point out that CIP-005-8 R1 Part 1.1 specifically denies '*Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement*' which does not meet the objective based model that the standards are supposed to now be written to. This very specifically identifies a technology that cannot be used to meet the requirement. This statement appears to be in conflict with the Technical Rationale for the ERC term.

ERC is no longer based on 'external' being defined in terms of the ESP as ESPs are changing in light of Zero Trust models. Zero Trust will shrink ESP's over time to the smallest, most granular object possible including a single device or possibly to process or resource level on a device.

Additionally, question #10 begins by asking about the revised CIP-005 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-005.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

•   R1.6 – Minnesota Power believes that the requirement is ambiguous and could be interpreted as traffic is only required to be monitored entering or leaving an ESP, but it could also be interpreted as traffic must be monitored both entering and leaving an ESP.

•   R2.1 - Minnesota Power believes the inclusion of "Intermediate Systems used to access Applicable Systems of Part 2.1" in the Applicable Systems section of Part 2.1 creates a recursive reference that will never resolve as it would require an Intermediate System be used to access another Intermediate System.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP in general agrees with the proposed changes to the NERC Glossary terms, except as indicated in our responses above.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

In support of NPCC RSC comments.

Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.”

Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts?

Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS.

Request correction of the typo “Systerms” in Part 2.6.2’s Requirements

Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties?

Overall comment: We suggest reviewing the word ‘’communications’’, it should be a bi-directional routable protocol or a routable protocol. Communication is too vague. One could imply that serial, layer 2 communication needs to be controlled. If the intent of the SDT is to broaden the scope, why keep the notion of bi-directional routable protocol or routable protocol.

Requirement 1.1 New concept is inserted “between intelligent electronic devices”, what is an intelligent electronic device? We propose the SDT to use Cyber Asset definition.

The note regarding Host-based firewalls, is in sync with the definition of ESP, except we don’t agree on imposing this limitation. Also, the firewall wording is not used in the language of the requirements, controlled communication is the usual wording. We suggest the removal of this note.

The requirement should use the same language that is used for the other requirements. Suggestion

Applicable Systems connected to a network via a routable protocol must be protected by an ESP that Permits only needed and controlled communications and denies all other communications.

Requirement 1.2 We suggest reviewing the measure column. MPLS is mainly a WAN protocol. Also, a network switch enforces the VLAN concept so the network switch would be an SCI and EACMS? We suggest that the SDT review the mechanism permitting the control of communication. Someone could build a complete ecosystem with only a network switch (BCA is on VLAN 2 and the permitted users are on VLAN 2, the denied users are on VLAN 3, all of this is managed and controlled by a network switch, a switch this is virtualized.

Requirement 1.3 introductions of network communication. For some requirement, communication is the only word used (1.1, 1.2), we suggest that the SDT review the usage of the word ‘’network’’ and be uniform within all standards.

Requirement 1.4: No Comments

Requirement 1.5 version 6 of this requirement is only applicable to BCA and PCA, in this version the SDT as added PACS hosted on SCI; and EACMS hosted on SCI, and SCI identified independently supporting an Applicable System above. One could understand why the SCI is part of the applicable systems but why did the SDT target PACS and EACMS. We suggest to the SDT to remove PACS and EACMS. Also the line “SCI identified independently supporting an Applicable System above” should be replaced by the usual language used throughout the requirements, i.e.” SCI identified independently supporting an Applicable System from Part 1.1.” Clarification to that sentence would also be welcome, are they “SCI identified independently” or are they “SCI that is identified to be supporting independently an Applicable System”.

Requirement 1.6, this requirement is valid in the context of the old ESP definition. In the context of the suggested definition, this is an additional requirement resulting in a burden for the entity. The SDT should evaluate the possibility of enforcing the ESP controls (permitted communication and malicious communications) directly on the cyber asset itself, an EACMS wouldn't be required. The BCA, PCA, EACMS, PACS, SCI could have their own controls (host firewall, host IDS, Host Endpoint controls).

Requirement 2.1 We suggest reviewing the Applicable column

EACMS that enforces an ESP for the Applicable Systems in Part 1.1.

This is an additional requirement resulting in an additional burden for the entity.

SCI identified independently supporting an Applicable System above

We suggest the normal wording (SCI identified independently supporting an Applicable System from Part 1.1.

Increase in the need for Intermediate System (EACMS used for the ESP, SCI).

Requirement 2.2 No Comments

Requirement 2.3 No Comments

Requirement 2.4 We suggest the SDT normalize the wording, ''from SCI identified independently supporting an Applicable System above'' to ''SCI identified independently supporting an Applicable System from Part 1.1''.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn't have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.5 We suggest the SDT normalize the wording, ''from SCI identified independently supporting an Applicable System above'' to ''SCI identified independently supporting an Applicable System from Part 1.1''.

Also, SDT proceeded in a change of scope for the Medium Impact BES Cyber Systems. In the previous version, ERC was a criteria. The suggested version doesn't have this criteria which will increase the scope of the requirements and the burden on the entities.

Requirement 2.6. Requirement 2.6.1 is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization or consolidating services like databases or web applications. We suggest the SDT review their objectives and how to implement them. The reference to Part 2.1 in 2.6 can also be confusing for the requirement, does the restriction in CPU and memory also apply to the SCI in 2.1 or only to the Intermediate Systems.

Requirement 2.6.2 should use the same language that is used for the other requirements. Suggestion

Permit only needed and controlled communications and denies all other communications between Intermediate Systems and Applicable Systems of Part 2.1.

Reference 2.6.1, Restrict VCAs of Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI

Reference 2.6.2. Permit only needed and controlled communications between Intermediate Systems and Applicable Systems of Part 2.1.

Requirement 3 Is this a new requirement part of the SAR?

Also, requirement 2.4 and Requirement 2.5 doesn't mention the ERC criteria for the Medium Impact BES Cyber Systems, yet requirements 3.1 and 3.2 mention the ERC criteria. This will increase the burden on the entities. We suggest the SDT review the scope and criteria.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	
Comment	
Cleco supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	No
Document Name	
Comment	
Remove Intermediate Systems from the applicability for 2.1 to permit authorized IRA through an Intermediate System (on the clean version). R1.1 – The last sentence in the requirement is prescriptive and would be more appropriate in the technical rationale document. Consider removing this and moving it to TR: “Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.” R2.1 – Revise as follows to improve readability - Permit authorized IRA to Applicable Systems only through an Intermediate System.	
Likes 0	
Dislikes 0	

Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
There is still there is a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication, but have not adequately enforced protections to ensure that the ports are not used by malicious actors – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to ensure validity of communications to Applicable Systems. CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters but no minimum level of encryption is required which could result in older less secure methods being used leaving the data at risk. CIP-005-8 depends upon approved SCI terminology and other definitions associated with virtualization as a whole. Approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

The definition for ESP remains incomplete. We would suggest altering the definition as follows: “A logical boundary defined by a set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System and that groups CIP Systems of the same or lower impact rating”	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We support NPCC TFIST's comments as found below: Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads “Permit only needed and controlled communications to and from Management Interfaces and deny all other communications” which seems to include Part 1.3 which reads “Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.” Request clarification on Parts 1.4 and 2.1. Does Applicable System “above” refer to the other items in this Applicable Systems or the above Requirements / Parts? Request additional language in Part 2.1 to make it obvious this is for IRA where the EACMS is the destination - - - not passing through the EACMS. Request correction of the typo “Systerms” in Part 2.6.2’s Requirements Request clarification on Exemption 4.2.3.3 which reads “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.” Does this exempt any entity including third parties?	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	No
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	

Likes 0

Dislikes 0

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

While the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the 'as is' state of the definitions associated with some of the proposed NERC Glossary terms per comments provided in this project comment/ballot submission.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE recommends that the SDT consider an approach by which SCI is “high watermarked” to whatever applicable systems they are hosting.

Texas RE is concerned that not requiring SCI hosting BCS to be categorized as BCS themselves will result in a reduced security posture for those SCI. A previous version of the Technical Rationale indicated that SCI would be sufficiently protected, stating “The SDT recognizes that SCI indeed has the same impact as a virtual BES Cyber Asset and even more so if hosting numerous BES Cyber Assets. For the first formal posting of all affected standards, the requirements for SCI will be equal to BCA and in fact be subjected to additional requirements due to its impact (e.g. CIP-005 R1 Part 1.6).” In this current posting, however, Texas RE noticed CIP-005 R1.1 and CIP-005 R1.4 do not include SCI within scope as applicable systems, which means SCI arguably may not fall within the full scope of the CIP standards.

Texas RE also notes that “Intermediate Systems use to access Applicable Systems of Part 2.1” are an applicable system of Part 2.1. CIP-005 R2.1 requires that IRA must go through an Intermediate System. This appears to require Registered Entities to use an Intermediate System (IS1) prior to accessing a separate Intermediate System (IS2) that will then be used to access other applicable systems, such as high or medium impact BCS. Texas RE inquires as to whether or not this is the SDT’s intent.

Likes 0

Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	No
Document Name	
Comment	

The proposed revised definition of IRA as written, Management Interfaces of SCI would appear to need to reside within an ESP and Management Interfaces of EACMS that enforce the ESP would also need to reside within an ESP. As a whole it is very difficult to understand the security objective. This seems very prescriptive, trying to introduce security that is perhaps outside the scope of virtualization.

SCI identified independently supporting an Applicable System. 1.1 - is communication protected both inbound and outbound or only inbound? 1.3 - isn't this the same as 1.2; if an entity is only permitting needed communications then wouldn't one be denying communications from high impact BCS and PCA?

In CIP-005 R1.2 it is not clear with “only needed and controlled communications.” Only needed communications seems clear but controlled communications does not seem clear. Is this referencing not routed traffic such as broadcast traffic?

For 1.4 SMUD would like to see "mitigate the risk to data traversing" instead of "Protect the data." This would allow for entities to use their own transport media rather than a third parties transport networks. Encryption should not be a required control in this environment where availability is the top priority. For CIP-005 R2.1 – An RE would need an intermediate system to access an intermediate system and also need an intermediate system to get to an EACMS that enforces and ESP?

It is unclear what a bi-directional routable protocol is. It seems that the definition itself would exclude serial devices that are being communicated to since technically the communication is uni-directional. A serial connection cannot have bi-directional routable communication using a routable protocol, this is wrong. There can be IRA, but there is no bi-directional communication using a routable protocol. Entities are forced to overlook the fact that this is technically not correct but continues to be misinterpreted to ensure that serial communication is kept in scope. SMUD does agree that this serial communication should be in scope, but changing the meaning of bi-directional routable protocol make it very difficult to understand from a networking perspective.

Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	

Comment

SIGE does not agree to the ESP definition as stated in SIGE's response to question 4. SIGE proposed the following definition for ESP:

"A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System and that groups CIP Systems of the same impact rating."

SIGE does not agree to the IRA definition as stated in SIGE's response to question 5. SIGE proposed the following definition for IRA:

"A user initiated real-time electronic access by a person from outside of a Responsible Entity's Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) to a CIP System within the Responsible Entity's ESP or PSP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System's user interfaces."

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA does not support the modified language in CIP-005. How SCI is to be independently identified is not clear.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CEHE does not agree to the ESP definition as stated in CEHE's response to question 4. CEHE proposed the following definition for ESP:

"A set of configurations or policies enforced by an EACMS that controls routable protocol communications to or from any part of a BES Cyber System and that groups CIP Systems of the same impact rating."

CEHE does not agree to the IRA definition as stated in CEHE's response to question 5. CEHE proposed the following definition for IRA:

“A user initiated real-time electronic access by a person from outside of a Responsible Entity’s Electronic Security Perimeter (ESP) or Physical Security Perimeter (PSP) to a CIP System within the Responsible Entity’s ESP or PSP, either directly or through another Cyber Asset or Virtual Cyber Asset for the purpose of connecting to any of the CIP System’s user interfaces.”

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Several of the terms and their usage, especially SCI, lends ambiguity with their use in the revised CIP-005 Standard. Further clarifications and refinements of the terms should be given attention.

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	

Comment

While mostly in agreement with the proposed changes, we note a possibility that with the revised ESP definition and revised verbiage of R1.1 that an interpretation could be made that an ESP is required around serial-only connections. Please revise requirement part verbiage accordingly to prevent this possible interpretation.

Additionally, question #10 begins by asking about the revised CIP-005 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-005.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No

Document Name	
Comment	
Need clarification for IRA and ERC . See comments for questions 3 and 5	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
See response to question 3, 5, and 6	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Consider adding ‘Virtual Cyber Asset’ context to the EAP definition, just as has been added to the EACMS definition. This would allow for Virtual Cyber Asset based firewalls and virtual firewall appliances to have an identified EAP as well. The inclusion of ‘Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement’ is not consistent with the proposed ESP definition. Consider the following - **EAP -** A policy enforcement point or a Cyber Asset, Virtual Cyber Asset interface that allows routable communication to and from the BES Cyber System within an Electronic Security Perimeter. The language ‘must be protected by an ESP that permits only…’ used in Part 1.1 appears to be out of context for an ESP, as defined. Wouldn’t it be an EACMS that is performing the electronic access control? This would be more consistent with the language use in the Applicable Systems of Part 1.6. Consider the following language -	

Applicable Systems connected to a network via a routable protocol must be (within an ESP and protected by an EACMS) ADD WORDS IN () that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices.

Specific to Part 1.2, the use of ‘controlled’ may create more ambiguity in meeting the security objective than intended. Also noting the use of ‘needed communications’ in Part 1.1, ‘controlled communications’ in Part 1.2 and ‘network communications’ in Part 1.3. Consider the following language –

Permit only needed and controlled communications to and from Management Interfaces, and deny all other communications.

Part 1.4, consider the use of ‘electronic controls’ to be consistent with the second bullet.

‘Electronic controls that ensure confidentiality and integrity (such as encryption), or…’

Part 2.1, the use of ‘Intermediate Systems used to access Applicable Systems of Part 2.1’ as an Applicable Systems does not appear to be consistent with the ESP definition as IRA to an IS does not include an IS.

Part 2.2, consider changing ‘client’ to ‘remote Cyber Asset’ or ‘remote client’ to the requirement –

Protect the confidentiality and integrity (e.g., encryption) of IRA between the (remote) ADD WORK IN () Cyber Asset and the Intermediate System.

Part 2.6, the inclusion ‘Intermediate Systems used to access Applicable Systems of Part 2.1’ appears to create a hall of mirrors, meaning an Intermediate System used to access an Intermediate System.

Part 2.6.2, suggest removing ‘controlled’ and only using ‘needed communications’ as has been used in other parts.

Permit only needed (and controlled) DELETE WORDS IN () communications between Intermediate Systems and Applicable Systems of Part 2.1.

Likes 0

Dislikes 0

Response

Josh Johnson - Lincoln Electric System - 1

Answer No

Document Name

Comment

We agree with the changes to the standard, however, the potential clarity issues that arise from the definition changes of ESP (and subsequently an EACMS) may cause unintended scoping regarding Registered Entities BCS in the field. See question 4 for further explanation and alternative proposal.

Likes 0

Dislikes 0

Response

Ronald Bender - Nebraska Public Power District - 5

Answer No

Document Name	

Comment

NERC Definition Changes -- Electronic Security Perimeter (ESP) - removed the routable protocol qualifier. Consider the following:

- The new ESP qualifier is an EACMS. The EACMS definition does not have a routable protocol/communication qualifier, and it references ESPs. It seems like a circular definition.
- When looking at the definitions only, it appears to require serial connected Cyber Assets have an EACMS to protect their serial communication links, however they are not required to have an Electronic Access Point (EAP) as the EAP definition has a routable communication qualifier.
- When assessing CIP-005-8 R1.1 the Requirements section qualifies ESPs are only required for Applicable Systems with routable protocols. It does not have a qualifier of ERC so if there is only ethernet within a system that never leaves an asset, an ESP is required even if you have no EAP. This is the same as V5 of the standards.
- If a BCA has both serial and Ethernet communications that leave an asset, auditors could require an EACMS for serial connections because a BCA that has routable protocol leaving an asset is required to have an ESP, and an ESP is required to have an EACMS. The same BCA serial that would leave the asset would require an EACMS because the ESP definition does not exclude serial communication. Not sure what type of device a serial EACMS would be.
- The SDT proposed definition creates ambiguity around serial communication configurations and whether they have to be documented as part of an ESP.

We recommend revising CIP-005-X R1 Part 1.1 to read:

Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other commuincations. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement. Excluding:

- Time sensitive protection or control functions between intelligent electronic devices
- Cyber Asset to Cyber Asset serial communication not meeting the IRA definition

We also want to point out that CIP-005-8 R1 Part 1.1 specifically denies '*Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement*' which does not meet the objective based model that the standards are supposed to now be written to. This very specifically identifies a technology that cannot be used to meet the requirement. This statement appears to be in conflict with the Technical Rationale for the ERC term.

ERC is no longer based on 'external' being defined in terms of the ESP as ESPs are changing in light of Zero Trust models. Zero Trust will shrink ESP's over time to the smallest, most granular object possible including a single device or possibly to process or resource level on a device.

Additionally, question #10 begins by asking about the revised CIP-005 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-005.

Likes 0	
Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5

Answer	No

Document Name	

Comment

See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

For Part 1.1, we suggest including the word “directly” in this phrase “connected directly to a network” for absolute clarity that serial devices do not require an ESP, regardless of any upstream protections afforded by the newly proposed IRA definition.

We also suggest that Part 1.1 be modified to remove the host-based language due to proposed inclusion in glossary term as described in response to Question 4.

We suggest aligning the Applicable Systems language in (current) Part 1.4 and (current) Part 1.6 using reference back to Part 1.1 with additional “at Control Centers” qualifier.

We suggest placing the “ESP outside PSP” requirement as the new Part 1.6 so that dial-up and malicious communications requirements maintain their current part numbers. This minor change would allow for continuity of evidence references that would otherwise be confusing and burdensome.

Inclusion of the ESP reference in the malicious communication requirement may present challenges for Zero Trust environments where an application layer firewall or IDS cannot be applied between each ESP. Language such as the following would allow for more flexible implementations that still meet the security objective of this requirement: “Detect known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP. Detection may occur at the boundary or as part of EACMS monitoring capabilities.”

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy does not agree with the proposed changes in CIP-005. Independly identified SCI is listed throughout the applicable systems column and with our concern with the lack of clarity in Independly identified SCI, we can not support at this time.

While Xcel Energy does not support the approval of this Standard at this time, we do support other aspects in the modifications made as identified in EEI comments.

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
See response to question #4.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
:No. Please see NRG's responses to questions 4 and 7.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	

No. Please see NRG's responses to questions 4 and 7.

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

In Reference to CIP-005-8

No – As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture. I have a request for additional information from the Standards Drafting Team to get clarity.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	No
Document Name	

Comment

Chelan agrees in principle with CIP-005, but there is a major flaw in CIP-005 R2. CIP-005-8 R2.1 includes "Intermediate Systems used to access Applicable Systems of Part 2.1" as part of the Applicable Systems. This language indicates that an Intermediate System is required to access an Intermediate System. Is this a typo? If not, additional clarification is requested. This appears to create a hall of mirrors.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

CIP-005-8 R1 Part 1.6 proposes the following:

Detect known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.

In light of the new ESP definition, perhaps this requirement should state: Detect known or suspected malicious Internet Protocol (IP) communications entering or leaving an applicable system.

In the alternative, the new definition of ESP would need further refinement. CIP-005-8 R1 Part 1.4 is another example where the language of the requirement appears to be using the approved ESP definition from CIP V5.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Tacoma Power agrees with the proposed changes to the NERC Glossary terms. However, we identified the following improvements and minor corrections to the CIP-005 documentation:

- Suggest simplifying the measures in CIP-005 R1 Part R1.1 by moving the following sentence into the opening statement: “that enforces an ESP electronic access control and logical isolation and documents the business need.”
- In CIP-005 R2 Part 2.1, a space is needed between “onlythrough”.
- In the clean version of CIP-005 R2 Part 2.1, the last statement in the Applicable Systems column, “Intermediate Systems used to access Applicable Systems of Part 2.1,” should be removed.
- Correct typo in CIP-005 R2 Part 2.6.2: “Systerms” should be “Systems”.

Likes 0	
Dislikes 0	

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer	Yes
Document Name	

Comment

SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
We support these approach used for these changes once acceptable definitions are in place.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS does not believe that Requirement R1.4 accounts for all of CIP-006, Requirement R1.10. There is a lack of associated PCAs in Requirement R1.4 that was contained within CIP-006 R1.10.	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

11. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	No
Document Name	

Comment

The changes to CIP-007 R1.1 and the conforming changes are appropriate. The new requirement CIP-007 R1.3 is too specific in requiring a specific technology be used. See comments in Q14 for comments on CIP-007 R1.3

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

See response to questions #1, #2, and #6.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy does not agree with the proposed changes in CIP-007. Independly identified SCI is listed throughout the applicable systems column and with our concern with the lack of clarity in Independly identified SCI, we can not support at this time.

While Xcel Energy does not support the approval of this Standard at this time, we do support other aspects in the modifications made as identified in EEI comments.

Likes 0	

Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
We support the proposed R1.3. We do not support the other changes to the standard. The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System. It is unclear why R1.2 Applicable Systems now include “Non-programmable communications components located inside both a PSP and ESP” for both high and medium impact.	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
See response to question 3, 6, and 8	

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	No
Document Name	

Comment

AZPS does not agree with the proposed changes in Requirement 1.2 and would like clarification on what “non-programmable communications components located inside both a PSP and ESP”includes.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Need clarification for SCI “identify independently”. See comment for question 2.

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	

Comment

The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System. It is unclear why R1.2 Applicable Systems now include “Non-programmable communications components located inside both a PSP and ESP” for both high and medium impact. Lastly, question #11 begins by asking about the revised CIP-007 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-007.

We are concerned about revising the existing CIP standards to address virtual technologies. We recommend any necessary requirements pertaining to security controls around virtual cyber assets used for a CIP function be encoded in a new Reliability Standard. Please see our comment on this in response to question #14.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Several of the terms and their usage, especially SCI, lends ambiguity with their use in the revised CIP-007 Standard. Further clarifications and refinements of the terms should be given attention.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree to the Management Interface definition as stated in CEHE's response to question 6. CEHE proposes the following definition: "A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems."	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	

Comment

NCPA does not support the modified language in CIP-007. How SCI is to be independently identified is not clear.

Likes 0

Dislikes 0

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

SIGE does not agree to the Management Interface definition as stated in SIGE's response to question 6. SIGE proposes the following definition:

"A user interface, logical interface or dedicated physical port, excluding touch controls (e.g., power switch, touch panel, etc.), that is used to: control the processes of initializing, deploying, and configuring or lights-out management capabilities of Cyber Systems."

Likes 0

Dislikes 0

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

While the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the 'as is' state of the SCI definition proposed in this project comment/ballot submission. Otherwise, the CIP-007 standard itself is largely unchanged and no other issues were identified.

Likes 0

Dislikes 0

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No

Document Name	
Comment	
We support NPCC TFIST's comments as found below: Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.” Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
The modification to the definition to ERC brings serially connected OT Devices using a protocol-converter into scope for multiple CIP-007 requirements. In some instances, compliance with all the CIP-007 requirements would be impossible. The use of a protocol converter does not facilitate centralized logging, review, and alarming (based on events). It simply facilitates data acquisition and IRA to these devices. We suggest not revising the definition of ERC, leaving the concept of a protocol break in place and require the protocol converter to either be categorized as a BCA, PCA or EACMS (depending on the circumstance). The serial OT device could still utilize the proposed definition for IRA to be in scope for CIP-005.	
Likes 0	
Dislikes 0	
Response	
Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE	
Answer	No
Document Name	
Comment	
OKGE supports EEI's comments.	
Likes 0	

Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

In support of NPCC RSC comments.

Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.”

Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency

Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.

Requirement 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA

We do not understand the change from Where technically feasible, enable only logical network accessible ports (previous version) to Enable only network-accessible Internet Protocol (IP) ports (suggested version). The introduction of IP is limiting. SDT should try to use routable protocol, Enable only network-accessible routable protocol ports.

Requirement 1.2 This new criteria for the applicable system, Non-programmable communication components located inside both a PSP and ESP is difficult to understand because the NERC CIP always treated cyber assets, the non-programmable were always excluded from the CIP standards. This is an increase in scope and doesn’t seem related to the virtualization project.

We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above.

Requirement 1.3 This requirement is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization. Thus, avoiding the sharing resources between non-CIP VCAs and CIP VCA doesn’t offer any benefits versus the current version. We suggest that the SDT review their objectives and how to implement them.

Requirements 2, 3, 4, 5 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

We disagree with the changes in CIP-007.

Recommendations:

- For CIP-007 R1.1 and R1.2, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

- For CIP-007 R1.3, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA.

- For CIP-007 R2.1, R2.2, R2.3 and R2.4, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

· For CIP-007 R3, R4, R5 and their Parts, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System. It is unclear why R1.2 Applicable Systems now include “Non-programmable communications components located inside both a PSP and ESP” for both high and medium impact.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.”

Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency

Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.

Requirement 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA

We do not understand the change from Where technically feasible, enable only logical network accessible ports (previous version) to Enable only network-accessible Internet Protocol (IP) ports (suggested version). The introduction of IP is limiting. SDT should try to use routable protocol, Enable only network-accessible routable protocol ports.

Requirement 1.2 This new criteria for the applicable system, Non-programmable communication components located inside both a PSP and ESP is difficult to understand because the NERC CIP always treated cyber assets, the non-programmable were always excluded from the CIP standards. This is an increase in scope and doesn’t seem related to the virtualization project.

We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above.

Requirement 1.3 This requirement is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization. Thus, avoiding the sharing resources between non-CIP VCAs and CIP VCA doesn’t offer any benefits versus the current version. We suggest that the SDT review their objectives and how to implement them.

Requirements 2, 3, 4, 5 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

R1.4 Applicablity is missing SCI that may be part of a BCS. As written, it implies that SCI as part of a BCS aren't subject to this requirement. Or is this an issue with clarity around CIP-002 or the actual definition? Is the idea the independently identified SCI is the only SCI with non-CIP Systems hosted on them. If so that needs to be made clear in CIP-002 or the definition. If not then the scope of R1.4 needs to include "SCI identified as part of a BES Cyber System, EACMS, or PACS" or possibly strike "identified independenty" so we get "SCI supporting:…"

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

The change to specification of "Internet Protocol ports" in proposed CIP-007-7 R1.1 supports technical restriction of protection to only a particular network technology. The prior language for CIP-007 R1.1 did not involve "Internet Protocol" ports and allowed for service identification to include one/more ports. ISO-NE requests either clarification of the intent regarding technical specification of networking technology for this case or reversion of the requirement language to support backward compatibility.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC

Answer	No
Document Name	

Comment

In support of IRC SRC/SWG.

Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.”

Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency

Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Please provide more clarity on Requirement 1.2

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

We disagree with the changes in CIP-007.

Recommendations:

- For CIP-007 R1.1 and R1.2, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.
- For CIP-007 R1.3, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA.

- For CIP-007 R2.1, R2.2, R2.3 and R2.4, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.
- For CIP-007 R3, R4, R5 and their Parts, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

o CIP-007 R1 – Please confirm the P1.1 Logical ports justification and details for serially connected CIP Systems are excluded but expectation of the physical wiring will be required for P1.2?

  o CIP-007 R4.2 – Please clarify the serial CIP System must now alert for failure of event logging.

o CIP-007 R5.6 – Please clarify a serial CIP System such as an RTU or Relay that was a BCA or PCA without ERC now with the proposed change requires the password change every 15 months?

Likes 0	
Dislikes 0	

Response

Cynthia Lee - Exelon - 5

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan

Answer	No
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	No
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1	
Answer	No
Document Name	
Comment	
Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.” Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.	
Likes 0	
Dislikes 0	
Response	

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	No
Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT supports the IRC SRC comments.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
EEI supports many of the proposed NERC Glossary terms, however, concerns remain with those terms identified in our comments above. EEI also notes that the phrase “SCI identified independently” is unclear in its intent and needs to be clarified before EEI can support the revisions to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No

Document Name	
Comment	
Agree with change to CIP-007. Do not agree with related NERC Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC. PJM requests additional clarity on what is considered a “non-programmable communication component”.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No

Document Name	

Comment

Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.”

Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency

Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.

Requirement 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA

We do not understand the change from Where technically feasible, enable only logical network accessible ports (previous version) to Enable only network-accessible Internet Protocol (IP) ports (suggested version). The introduction of IP is limiting. SDT should try to use routable protocol, Enable only network-accessible routable protocol ports.

Requirement 1.2 This new criteria for the applicable system, Non-programmable communication components located inside both a PSP and ESP is difficult to understand because the NERC CIP always treated cyber assets, the non-programmable were always excluded from the CIP standards. This is an increase in scope and doesn’t seem related to the virtualization project.

We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above.

Requirement 1.3 This requirement is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU power, memory, etc.). Enforcing restriction of those types limits the possible gain of instating virtualization. Thus, avoiding the sharing resources between non-CIP VCAs and CIP VCA doesn’t offer any benefits versus the current version. We suggest that the SDT review their objectives and how to implement them.

Requirements 2, 3, 4, 5 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above To SCI identified independently supporting a High Impact BC, Medium Impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST believes Requirement R1 Part 1.3 (“Prevent the sharing of the CPU and memory,…”) should apply to SCI identified independently and to SCI that are grouped into BES Cyber Systems.

N&ST also believes Requirement R1 Part 1.3 should be slightly revised for better clarity. We suggest, “Prevent the sharing of the CPU, memory, and Management Interfaces of SCI with non-CIP Systems.”	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)	
Answer	No
Document Name	
Comment	
Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to “Internet Protocol ports” instead of “ports.” Request clarification on the inconsistency between CIP-007 Parts 1.1 and 1.2. 1.1 uses “Internet Protocol ports” while 1.2 uses “physical input/output ports” and “network connectivity.” We expected consistency. Request explicit language in CIP-007 R2 that these patching Requirement do not include patching in the cloud. We understand that the SAR does not include cloud connectivity.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes

Document Name	
Comment	
Duke Energy agrees with the proposed CIP-007 strategy and notes that several definition concerns are identified in response to other Questions.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Part 1.1, consider removing 'by the Responsible Entity' as it is already stated in R1, 'Each Responsible Entity shall…' Part 1.3, the use of 'Management Interfaces' in the requirement is redundant with the definition of SCI. Consider changing to the following - Prevent the sharing of the CPU and memory of Applicable Systems (Management Interfaces of SCI) DELETE WORDS IN () with non-CIP Systems.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
We support these approach used for these changes once acceptable definitions are in place.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes

Document Name	
Comment	
ACES agrees with the changes made based on industry comments, but regarding R2, based on webinar and technical rationale documentation, dormant VCAs are not considered Applicable Systems until they become “active” instances again. How is this going to be handled if an entity’s SCI automatically spins up dormant VCA’s when needed, how would an entity track and document the controls necessary prior to being an active VCA? Allowing automatic remediation of non-responsive VCAs is a benefit to utilizing virtualization and could cause an entity to be out of strict compliance. Also, wouldn’t a dormant instance previously a VCA, which could be a VCA in the future that has not been “connected” to the BCS for 30 consecutive days be considered a TCA? ACES feels like there needs to be VERY clear guidance on how to keep dormant VCAs compliant, that aren’t actually in scope when dormant and if dormant for greater than 30 days constitutes a VCA as a TCA. In our opinion an in scope VCA, dormant or not, should always remain in scope until retired. Virtualized environments are highly dynamic, thus the standards should have considerations for such capabilities. AEPC has signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	
Answer	Yes
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	

Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Although we agree with returning back to looking at ports and not just services the updated language uses the term “Internet Protocol (IP) Ports”. Under Internet Protocol (IP), the transport layers (e.g. TCP, UDP) create and maintain the ports for the underlying services. The Internet Protocol is the network layer, which uses the host address to communicate. Consider alternate verbiage.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
We agree with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
See MidAmerican Energy Company comments from Darnez Gresham.	

Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports many of the proposed NERC Glossary terms, however, concerns remain with those terms identified in our comments above.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
We agree with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
We support the proposed R1.3. The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System. It is unclear why R1.2 Applicable Systems now include “Non-programmable communications components located inside both a PSP and ESP” for both high and medium impact.	
Likes 0	

Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

ACES agrees with the changes made based on industry comments, but regarding R2, based on webinar and technical rationale documentation, dormant VCAs are not considered Applicable Systems until they become “active” instances again. How is this going to be handled if an entity’s SCI automatically spins up dormant VCA’s when needed, how would an entity track and document the controls necessary prior to being an active VCA? Allowing automatic remediation of non-responsive VCAs is a benefit to utilizing virtualization and could cause an entity to be out of strict compliance.

Also, wouldn’t a dormant instance previously a VCA, which could be a VCA in the future that has not been “connected” to the BCS for 30 consecutive days be considered a TCA? ACES feels like there needs to be VERY clear guidance on how to keep dormant VCAs compliant, that aren’t actually in scope when dormant and if dormant for greater than 30 days constitutes a VCA as a TCA. In our opinion an in scope VCA, dormant or not, should always remain in scope until retired. Virtualized environments are highly dynamic, thus the standards should have considerations for such capabilities.

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	Yes
Document Name	

Comment

No comments

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern agrees with the proposed changes to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino	
Answer	
Document Name	
Comment	
It is not clear what is meant by SCI identified independently supporting an Applicable System. The wording “identified independently” is not clear.	
Likes 0	
Dislikes 0	
Response	

12. The SDT revised CIP-010 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

Dan Zollner - Portland General Electric Co. - 3

Answer	No
Document Name	

Comment

Portland General Electric Company supports most changes, but has concerns regarding changes to the TCA definition and applicability language in R4. In the current CIP-010-2 Standard, R4 clearly limits scope to High Impact and Medium Impact BES Cyber Systems and their associated PCAs. The proposed modification to the Standard appears to only exclude Low Impact BES Cyber Systems and supporting SCI. This implies that EACMS and PACS may now also be in scope. Based on the proposed definition of TCA, any Cyber Asset or VCA that meets the first three qualifiers and is connected for 30 consecutive calendar days or less to any Shared Cyber Infrastructure (including SCI that is only supporting a PACS or EACMS) is in scope for R4. This appears to be a fairly significant change in scope. Portland General Electric Company wonders if this was the drafting team's intent. If not, changing "Shared Cyber Infrastructure" to "Shared Cyber Infrastructure supporting a BES Cyber System" may resolve this. Additionally, clearly identifying scope within the R4 language (i.e. high impact and medium impact BES Cyber Systems, associated Protected Cyber Assets, and supporting SCI) may reduce confusion about the applicability of R4.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching?

We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable.

Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation.

Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope?

Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration?

Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

N&ST believes proposed changes beyond those needed for conformance:
Have little or nothing to do with virtualization,
Are unlikely to improve anyone’s cyber security posture,
Are outside the scope of the original 2016 SAR,
Are not addressed in any relevant FERC Order, and
Would be an unnecessary and unwelcome distraction for entities trying to adjust their CIP programs and documentation to accommodate new virtualization-related requirements.

Likes 0	
Dislikes 0	

Response

Ryan Olson - Portland General Electric Co. - 5	
Answer	No
Document Name	
Comment	
Portland General Electric Company supports most changes, but has concerns regarding changes to the TCA definition and applicability language in R4. In the current CIP-010-2 Standard, R4 clearly limits scope to High Impact and Medium Impact BES Cyber Systems and their associated PCAs. The proposed modification to the Standard appears to only exclude Low Impact BES Cyber Systems and supporting SCI. This implies that EACMS and PACS may now also be in scope. Based on the proposed definition of TCA, any Cyber Asset or VCA that meets the first three qualifiers and is connected for 30 consecutive calendar days or less to any Shared Cyber Infrastructure (including SCI that is only supporting a PACS or EACMS) is in scope for R4. This appears to be a fairly significant change in scope. Portland General Electric Company wonders if this was the drafting team's intent. If not, changing "Shared Cyber Infrastructure" to "Shared Cyber Infrastructure supporting a BES Cyber System" may resolve this. Additionally, clearly identifying scope within the R4 language (i.e. high impact and medium impact BES Cyber Systems, associated Protected Cyber Assets, and supporting SCI) may reduce confusion about the applicability of R4.	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System” Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching? We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable. Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation. Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope? Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration? Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions	

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Requirements 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above, SDT should be more precise. Requirement 1.1.5 (.1.5. Any security patches applied.) was removed, yet the measure “Documentation of authorization for cybersecurity patches implementation” was added as evidence of change authorization for security patches. Need for clarification as the change seems contradictory.

We suggest that the SDT review the wording of requirement 1.1.1. Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems; or firmware; This requirement mention ‘’images’’, why not use the word ‘’container’’?

Requirement 1.2 The overall requirement is questionable. Enforcing restrictions on the sharing of CPU or memory between systems limits the possible gain of instating virtualization. Also following the new definition of ESP, the latter is enforced by an EACMS and not by the SCI. We suggest that the SDT reviews their objectives and how to implement them.

Requirement 1.3 To be coherent shouldn't this requirement refer also to 1.2. After all, the CPU and memory controls are CIP-007 and the ESP is CIP-005. Follow the same logic as 1.4, i.e. ‘’for each change to the items listed in Part 1.1 or Part 1.2’’.

Requirement 1.4 no comments

Requirement 1.5 Our understanding is that we don’t need to verify the source nor the integrity of the security patches any longer. Since CIP-007 Patch management does not include those checks, wouldn’t this be considered as neglecting a compliance sound practice? (To validate the security patches)? Is this the real intent of the SDT?

Requirement 2.1 no comments

Requirement 3.3 What does ‘’Prior to becoming a new Applicable System” means?

We suggest that the SDT defines ‘’becoming’’. Is the intent of the SDT to permit the creation of a virtual cyber asset on an SCI, this SCI being in a production environment? We suggest that the SDT review the usage of ‘’production environment’’ versus ‘’becoming’’.

There is a need for additional clarification for “same type” in “like replacements of the same type of Cyber System”. Is ‘’type’’ associated with the Cyber System definition?

Since the baseline configuration doesn’t exist anymore, what is the intent of the SDT with the usage of the word ‘’configuration’’? How does one entity define configuration?

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer	No
Document Name	

Comment

SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	

Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the SWG. PJM requests to further define firmware (ex: does include BIOS and UEFI?) and provide implementation guidance for application containers.	
Likes 0	
Dislikes 0	
Response	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	

The requirement to “Authorize changes to 1.1.5 Security patches applied” was removed per the Technical Rationale that these changes would be included to changes to OS/Firmware or software, which Entergy agrees. However, the measures were explicitly updated to include “Documentation of authorization for cyber security patch implementation.” Calling out cyber security patches under this measure of authorization outside of a “change request record” as opposed to applying it to the other items may cause confusion regarding differing expectations for cyber security patches. This statement should be more generalized for the other CIP-010 R1.1 items as well.

Agree with change to CIP-010. Do not agree with Glossary of Terms

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI supports many of the proposed NERC Glossary terms, however, concerns remain with those terms identified in our comments above. EEI also notes that the phrase “SCI identified independently” is unclear in its intent and needs to be clarified before EEI can support the revisions to CIP-010. For this and the following concerns we cannot support the proposed changes at this time

1) Subpart 1.2.2 could be interpreted to allow mixed trust. The language does not provide sufficient clarity to ensure mixed trust is not allowed.

2) There is a typo in the Applicable Systems part of Requirement 2, Part 2.1, Table R2. SCI is incorrectly identified as CI.

3) Attachment 1 – Section 3; Removable Media; Part 3.2: the removal of language identifying high impact or medium impact BES Cyber Systems appears to expand this obligation beyond its original intent. EEI recommends that the original language be restored.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT supports the IRC SRC comments and offers these additional comments:

- ERCOT appreciates the removal of part 1.1.5 from the requirement language since patches would be covered under parts 1.1.1 and 1.1.2. However, the measure should be updated to be consistent with the requirement language.

- For Part 3.3, the requirement to build outside of the production environment and perform the vulnerability scan has been removed.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern agrees with the overall concepts but has several specific issues with the language.

In R1.1.1 the last "or firmware;" seems to be in error as firmware has already been covered in the list. The measures for this requirement could also use examples of evidence in regards to parent/child images such as VDI.

In R1.1.3 'including-applications containers' should be 'including application containers'

In R1.1.4 by including SCI in applicability, is the intent to know and authorize change to the SCI underlay communications at the IP port level? Typically the SCI underlay is service level due to the proprietary nature of the communication protocols, but 1.1.4 only allows services if one is unable to determine ports. Since you can always determine port numbers in use, this requires authorizing changes to port numbers within the underlay and not services, which may not be possible or of no value.

Also R1.1.4 could be improved by clarifying that the authorization is for a change to the OS, software, or configuration that subsequently will change ports or port ranges. Port numbers may be dynamically changing in real-time during process execution and further clarity around the level of change authorization intended is needed. As currently worded, a change authorization could be required every time a logical port is opened or closed by an executing process.

In R3.3, it would be clearer to state "Perform an active vulnerability assessment of a new Applicable System prior to it becoming a new Applicable System…" We suggest it helps with clarity to lead with the main required action and then follow it with the timing aspect of the 'prior to' phrasing rather than leading with it.

In R4, the scoping is set to “not lows”, which includes everything outside of CIP scope. The scoping has been removed from Attachment 1 as well, leaving the scoping for this requirement within the glossary definitions of TCA and RM. While this works, we’d prefer the scoping to be in the requirements within the standard.

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	No

Document Name

Comment

AWS agrees with changes to CIP-010 R1, R2, and R3. CIP-010 R4 has been updated to accommodate Virtual Cyber Assets and virtual machines hosted on physical Transient Cyber Assets, but because the standard language allows a Responsible Entity to choose one or a combination of security controls there may be security control gaps.

Since the TCA definition explicitly states that a VM running on a physical TCA can be treated as software running on the physical TCA, the VMs could be vulnerable to security threats undetected by the physical host. The Standard does not require additional security controls to be applied to the VMs running on physical TCAs.

We propose removing the language “Virtual machines hosted on a physical TCA can be treated as software on that physical TCA” from the TCA definition, and modifying the VCA definition to read, “A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure, a PCA, or a TCA.”

Likes 0

Dislikes 0

Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE

Answer No

Document Name

Comment

<duplicate>

Likes 0

Dislikes 0

Response

Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1

Answer No

Document Name

Comment

Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching?

We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable.

Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation.

Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope?

Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration?

Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Likes 0	
Dislikes 0	

Response

David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan

Answer	No
Document Name	

Comment

OPG concurs with NPCC's RSC comments

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- The complete removal of the term “baseline” creates a gap for the change management of Cyber Systems, similar to the removal of “ESP” that was re-instated. Recommend in CIP-010 R1 P1.1 allow for the continuation of “Baselines” at least in the measure as an option if not within the standard language.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

We disagree with the changes in CIP-010.

Recommendations:

- For CIP-010 R1.1, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.
- For CIP-010 R1.2, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA.
- For CIP-010 R1.3, R1.4 and R1.5, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.
- For CIP-010 R2, R3, R4 and their Parts, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

See what SRP stated in Question 2 and 11. Needs more clarity.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	

In support of IRC SRC/SWG.

Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching?

We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable.

Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation.

Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope?

Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration?

Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 3	
Answer	No
Document Name	
Comment	

GRE agrees with the comments submitted by the NSRF.

Likes 0	
Dislikes 0	

Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
ISO-NE requests greater clarification regarding the phrase in CIP-010-5 R3.3 "Prior to becoming a new Applicable System...". Does this mean when a Cyber Asset receives categorization per CIP-002 or some later phase of the deployment lifecycle? Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System” Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching? We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable. Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation. Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope? Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration? Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions	

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Requirements 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above, SDT should be more precise. Requirement 1.1.5 (.1.5. Any security patches applied.) was removed, yet the measure “Documentation of authorization for cybersecurity patches implementation” was added as evidence of change authorization for security patches. Need for clarification as the change seems contradictory.

We suggest that the SDT review the wording of requirement 1.1.1. Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems; or firmware; This requirement mention ‘’images’’, why not use the word ‘’container’’?

Requirement 1.2 The overall requirement is questionable. Enforcing restrictions on the sharing of CPU or memory between systems limits the possible gain of instating virtualization. Also following the new definition of ESP, the latter is enforced by an EACMS and not by the SCI. We suggest that the SDT reviews their objectives and how to implement them.

Requirement 1.3 To be coherent shouldn't this requirement refer also to 1.2. After all, the CPU and memory controls are CIP-007 and the ESP is CIP-005. Follow the same logic as 1.4, i.e. ‘’for each change to the items listed in Part 1.1 or Part 1.2’’.

Requirement 1.4 no comments

Requirement 1.5 Our understanding is that we don’t need to verify the source nor the integrity of the security patches any longer. Since CIP-007 Patch management does not include those checks, wouldn’t this be considered as neglecting a compliance sound practice? (To validate the security patches)? Is this the real intent of the SDT?

Requirement 2.1 no comments

Requirement 3.3 What does ‘’Prior to becoming a new Applicable System” means?

We suggest that the SDT defines ‘’becoming’’. Is the intent of the SDT to permit the creation of a virtual cyber asset on an SCI, this SCI being in a production environment? We suggest that the SDT review the usage of ‘’production environment’’ versus ‘’becoming’’.

There is a need for additional clarification for “same type” in “like replacements of the same type of Cyber System”. Is ‘’type’’ associated with the Cyber System definition?

Since the baseline configuration doesn’t exist anymore, what is the intent of the SDT with the usage of the word ‘’configuration’’? How does one entity define configuration?

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments 1:

We disagree with the changes in CIP-010.

Recommendations:

· For CIP-010 R1.1, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

· For CIP-010 R1.2, resulting from our proposed changes to the definition of PCA, this requirement is no longer needed since a non-CIP VCA sharing resources with any CIP Cyber Assets (BCA, EACMS, PACS or PCA) will be identified as a PCA.

· For CIP-010 R1.3, R1.4 and R1.5, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

· For CIP-010 R2, R3, R4 and their Parts, resulting from our proposed changes to the definitions, we suggest removing SCI language from the Applicable Systems.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

· R1.1 – application containers is not a well-defined term and should be clarified if it is going to be used in the Standards.

· R1.1 - The addition of “Documentation of authorization for cyber security patch implementation” into the Measures does not align with the removal of “Security patches applied” from the requirements of Part 1.1

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

In support of NPCC RSC comments.

Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching?

We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable.

Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation.

Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope?

Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration?

Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Requirements 1.1 We suggest that SDT normalize the wording, from SCI identified independently supporting an Applicable System above, SDT should be more precise. Requirement 1.1.5 (.1.5. Any security patches applied.) was removed, yet the measure “Documentation of authorization for cybersecurity patches implementation” was added as evidence of change authorization for security patches. Need for clarification as the change seems contradictory.

We suggest that the SDT review the wording of requirement 1.1.1. Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems; or firmware; This requirement mention ‘’images’’, why not use the word ‘’container’’?

Requirement 1.2 The overall requirement is questionable. Enforcing restrictions on the sharing of CPU or memory between systems limits the possible gain of instating virtualization. Also following the new definition of ESP, the latter is enforced by an EACMS and not by the SCI. We suggest that the SDT reviews their objectives and how to implement them.

Requirement 1.3 To be coherent shouldn't this requirement refer also to 1.2. After all, the CPU and memory controls are CIP-007 and the ESP is CIP-005. Follow the same logic as 1.4, i.e. ‘’for each change to the items listed in Part 1.1 or Part 1.2’’.

Requirement 1.4 no comments

Requirement 1.5 Our understanding is that we don’t need to verify the source nor the integrity of the security patches any longer. Since CIP-007 Patch management does not include those checks, wouldn’t this be considered as neglecting a compliance sound practice? (To validate the security patches)? Is this the real intent of the SDT?

Requirement 2.1 no comments

Requirement 3.3 What does ‘’Prior to becoming a new Applicable System” means?

We suggest that the SDT defines ''becoming''. Is the intent of the SDT to permit the creation of a virtual cyber asset on an SCI, this SCI being in a production environment? We suggest that the SDT review the usage of ''production environment'' versus ''becoming''.

There is a need for additional clarification for “same type” in “like replacements of the same type of Cyber System”. Is ''type'' associated with the Cyber System definition?

Since the baseline configuration doesn’t exist anymore, what is the intent of the SDT with the usage of the word ''configuration''? How does one entity define configuration?

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

R1-Removing baseline configuration does not change what needs to be done in practice. Entities will still need to retain a baseline configuration as evidence from which to establish the changes that were authorized.

- For Part 1.4 an entity will still need to show the baseline configuration prior to the change to show required cyber security controls in CIP-005 and CIP-007 are not adversely affected.

- For Part 2.1 an entity will still need to provide baseline configurations for evidence that they monitor at least once every 35 calendar days for unauthorized changes to the items listed Parts 1.1 and 1.2.

R3- The concern is that Remediation VLANs should be properly defined in the technical rational or Glossary as it may introduce situations where an entity could inadvertently place production Cyber Assets in this VLAN.

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

OKGE supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer	No
Document Name	

Comment

We support NPCC TFIST's comments as found below:

Suggest this Applicable Systems language can be misinterpreted – “SCI identified independently supporting an Applicable System.” Recommend clarification. Suggest adding a comma to distinguish between “identified independently” and “supporting.” Resulting in “SCI identified independently, supporting an Applicable System”

Request clarification of Requirement 1.1.1. Why is the lack of operating system relevant to patching?

We believe 1.1.4 will be hard to manage dynamic ports. We suggest managing (authorizing) by port (service) ranges is more manageable.

Request clarification of 3.3. The existing language allows for a noticeable time gap between the vulnerability assessment and becoming an Applicable System. If there is an expectation of the scan and the deployed state, we request an explicit expectation.

Request clarification of 3.3. What is the expectation of the timeline for devices that are in production and become in scope?

Since CIP-010 no longer includes a baseline, Part 3.3 Requirement of “like” and “type” seems loose. Request clarification. Does the entity define like, type and/or configuration?

Request three clarification on R4. 1) request clarification that this scoping applies to both TCAs and Removeable Media instead of TCAs and/or Removeable Media; 2) Request clarification on the applicable systems since this Requirement is different than others. Other Requirements identify applicable systems in scope. This Requirement identifies what is not in scope; 3) Request confirmation that this Requirement’s scoping is in the definitions

Request removal of the second bullet in 1.3 of Attachment 1 since freezing an OS does not protect against a vulnerability. This bullet does not belong in 1.3 (vulnerability). The intent seems to be preventing malicious code which is 1.4.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

Per CIP-010 R1, Part 1.1, the requirement to authorize all changes is very broad in terms of reference to OS, software applications, logical network accessible ports, etc. Per the strict language of the proposed standard, it is not clear what constitutes a change. Does the modification of a desktop background constitute an OS change? While it is expected the SDT intended to limit the nature of changes to versions or upgrades of OS and software and patches for example, the chosen language leaves this open to interpretation.

BC Hydro recommends adding more clarity here with the language of the standard. The Technical Rationale is not used as actual compliance guidance as indicated by NERC and without explicit language in the standard or without an endorsed compliance guidance document to supplement, the SDT's intent will be subject to the interpretation of audit entities. Also, it is not clear if these changes to be authorized are restricted only to changes to pre-existing CIP Systems or as part of the commissioning of a new CIP System.

While the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the 'as is' state of the SCI definition proposed in this project comment/ballot submission.

Attachment 1 to CIP-010 covering TCA and RM requirements have removed any context of what RM is expected to be connected to. It is not clear if the SDT intended for this removal to imply connection to any CIP System or to any non-CIP System? Recommend restoring the deleted text which referenced high and medium impact BES Cyber Systems, PCAs, and associated networks but to also include applicable SCIs, etc.to provide context.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No
Document Name	

Comment

The last proposed draft by this SDT of the Standards, though it used far more new definitions, seemed clearer. It's not clear what the existing changes are solving, nor is it clear what part(s) of the glossary of terms this question is addressing.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA does not support the modified language in CIP-010. How SCI is to be independently identified is not clear.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)

Answer	No
Document Name	

Comment

Comments:

R1.1:

Could the SDT explain why the security patches were removed?

What measures are in place to include alternate changes?

R1.2:

Is the SDT not including non CIP Assests to bring in all assets into the program by default?

Definitions:

Recommend the SDT provide an interpretation of the definition for Self-Contained Application. As written, the definition seems confusing, and could have the potential to be misinterpreted.

Recommend the SDT define and provide an interpretation in the scope of what it means by “Authorized Changes”.

R1.4 and R1.5:

Is the SDT asking for entities to include both firmware and OS? In the past, entities could not show firmware if an OS was present. This has the potential to broaden the scope, and includes authorized changes to the OS. Any changes to the OS would be included in scope and would have to be tested as part of 1.4 and 1.5. In the past, if the baseline was not changed, then the entity would not have concern about R1.4 and 1.5. This new standard will change that, and potentially add additional work for entities when a change is made. This could open entities to an investment in new tools because baseline is being removed.

R2.1:

Recommend defining in each subpart what is the change.

These changes seem broader than virtualization, is this in line with scope of the SAR?

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Several of the terms and their usage, especially SCI, lends ambiguity with their use in the revised CIP-010 Standard. Further clarifications and refinements of the terms should be given attention.

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	

Comment

The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System. Additionally, question #12 begins by asking about the revised CIP-010 but then asks about proposed changes to the NERC Glossary terms. We presume that this is a typo and that the question was about CIP-010.

We are concerned about revising the existing CIP standards to address virtual technologies. We recommend any necessary requirements pertaining to change management of virtual cyber assets used for a CIP function be encoded in a new Reliability Standard. Please see our comment on this in response to question #14.

Likes 0	
Dislikes 0	

Response
Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment
In R1.1.1, need for clarification as to the meaning of "…images used to derive operating systems". In Measures of R1.1, "Documentation of authorization for cyber security patches implementation" was added as evidence of change authorization for security patches, but the requirement for authorize change to security patches (formerly 1.1.5) was removed. Need for clarification as the change seems contradictory. In R1.5, need for clarification as to why prior to a change associated with security patches (formerly 1.1.5) was removed. In R1.3, since changes to SCI Configuration mentioned in R1.2 may impact CIP-005 controls, R1.2 should also be included similarly to R1.4 "For each change to the items listed in Part 1.1 or Part 1.2". In R3.3, need for clarification for "same type" in "…like replacements of the same type of Cyber System…"

Likes 0	
Dislikes 0	

Response
Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	No
Document Name	

Comment
AZPS agrees with EEI's comments on the repeated use of the undefined term "application container" causing confusion, as well as Attachment 1 – Section 3; Removable Media; Part 3.2: the removal of language identifying high impact or medium impact BES Cyber Systems appears to expand this obligation beyond its original intent. AZPS recommends that the original language be restored.

Likes 0	

Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	
See response to question 6 and 8.	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
We support the changes to the Requirements and Measures of R3.3. The phrase “SCI identified independently supporting an Applicable System” is confusing and not entirely clear if needed rather than just revise existing definition of BES Cyber System.	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	
Dislikes 0	
Response	

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	No
Document Name	

Comment

Duke Energy generally agrees with the approach enumerated by the SDT but notes that the inclusion of “application containers” must be addressed in the Technical Rationale document if it remains an undefined term. There is currently no explanation for this inclusion, leaving RE’s subject to auditor interpretation. Additionally, subpart 1.2.2 seems unnecessarily constrained and should likely include all changes to configuration that enforces an ESP.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy does not agree with the proposed changes in CIP-010. Independly identified SCI is listed throughout the applicable systems column and with our concern with the lack of clarity in Independly identified SCI, we can not support at this time.

While Xcel Energy does not support the approval of this Standard at this time, we do support other aspects in the modifications made as identified in EEI comments.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

There is insufficient clarity to ensure consistent outcomes in monitoring security controls.

Likes 0	
Dislikes 0	

Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	
No. Please see NRG's response to question 2 for additional detail.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
No. Please see NRG's response to question 2 for additional detail	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	
Comment	
CIP-010 R3.3 – Reclamation recommends adjusting the language. From: "Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for:". To: "Prior to the Entity commissioning a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for:".	
Likes 0	
Dislikes 0	

Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	Yes
Document Name	
Comment	
ACES agrees with the proposed changes to CIP-010 as long as “SCI identified independently…” is clarified based on question #2.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC recommends that CIP-010 be reviewed to ensure consistent usage of he acronym “BCS” versus BES Cyber System. Additionally, the proposed language in CIP-010 R 1.1.2 to include and address ‘application containers’ is confusing and unlikely to lead to the expected protections. Neither CIP-010 nor the proposed definitions address the definition of or criteria determinative of an “application container.” Additionally, the technical rationale also does not address what such ‘application containers’ consist of or provide language or criteria defining them. Accordingly, GSOC recommends providing additional defining language around the nature and scope of such ‘application containers.’

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Tacoma Power supports the proposed language, and has the following recommended edits:

- For CIP-010 R1.2, change language in the Applicable Systems column to match the Applicable Systems language used in CIP-007 R1.3
- Consider using a clearer or more commonly referenced word other than “instantiation” in CIP-010 R3.4 measures
- Correct typo in the second bullet in CIP-010 R3.4 measures: “Documention” should be “Documentation”
- For CIP-010 Attachment 1, Section 1.3 and 1.4, re-word the second bullet to state “Controls that maintain the last known good state of...”
- For CIP-010 Attachment 1, Section 2.2, re-word the fourth bullet to state “Review of controls that maintain the last known good state of...”
- Remove the “;” at the end of R1 Part 1.1.1 “; or firmware;” The reference here is back to the disk image used to derive, not stand alone firmware. So 1.1.1 should read: “1.1.1. Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems or firmware;”

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	Yes
Document Name	

Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

AEP supports the changes but has identified the following concerns:

- The repeated use of the undefined term “application container” could cause confusion. Given this term is an important part of CIP-007 Requirements, it should be defined.
- AEP does not support the need for the note in requirement 1.5 under Applicable Systems. We were not able to rationalize the note in Requirement 1.5 to contracts and thereby suggest removal of this note.
- There is a typo in the Applicable Systems part of Requirement 2, Part 2.1, Table R2. SCI is incorrectly identified as CI.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	Yes
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer	Yes
Document Name	

Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE agrees with the proposed definition for TCA.	
Likes 0	
Dislikes 0	
Response	
Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	
Comment	

CEHE agrees with the proposed definition for TCA.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
ACES agrees with the proposed changes to CIP-010 as long as “SCI identified independently…” is clarified based on question #2. AEPC signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
We support these approach used for these changes once acceptable definitions are in place.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	

Comment

Part 1.3, should ‘applications containers’ be changed to ‘application containers?’

Part 1.1.4, suggest changing language to be consistent with CIP-007-7, Part 1.1 –

Any network accessible Internet Protocol (IP) ports (or services if unable to determine ports).

Part 1.2.1, would it better scope the ‘system’ was changed to CIP Systems.

Controls sharing of CPU or memory between (systems)DELETE (CIP Systems)ADD with different impact ratings, including non-CIP Systems, hosted on SCI; and

Part 3.3, first bullet – would it be more accurately scoped to change ‘Cyber System’ to CIP System?

like replacements of the same type of CIP System with a configuration of the previous or other existing CIP System; or

Likes 0

Dislikes 0

Response

Josh Johnson - Lincoln Electric System - 1

Answer Yes

Document Name

Comment

We agree with the proposed changes to CIP-010. Does CIP-010 R1.3 intentionally not apply to changes made to items listed in Part 1.2?

Likes 0

Dislikes 0

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer Yes

Document Name

Comment

Chelan approves of the changes to CIP-010.

Likes 0

Dislikes 0

Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE noticed that proposed CIP-010 R4 language references the definitions of Transient Cyber Assets (TCA) and Removeable Media to define in scope devices for the requirement R4. For purposes of clarity, Texas RE recommends revising the requirement language to indicate which devices are in scope within the requirement language itself. Texas RE proposes the following language:

Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented processes that include each of the applicable requirement parts in Table CIP-010-x Table R4:

Applicable Systems

High Impact BCS and their associated:

1. SCI; and

2. PCA

Medium Impact BCS and their associated:

1. SCI; and

2. PCA

Requirement 4 Part 1

One or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1, except for use on low impact BCS or SCI supporting only low impact BCS(s).

Additionally, Texas RE continues to be concerned that security obligations will be reduced by removing the reference to baseline configurations. Establishing and maintaining baseline configurations represent best practices for system hardening. Texas RE recommends adhering to NIST Special Publication 800-53 (Rev. 5), CM-2 Baseline Configuration, which states, "*Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-*

upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture.”	
Likes 0	
Dislikes 0	
Response	

13. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 (conforming changes) based on industry comments. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Please refer to Dominion Energy's response Q14C below regarding CIP-004 and ERC as well as our comments to Q1.

There appears to be ambiguity on whether this pull in EACMS devices because of SCI? Clarity is needed.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

No. Please see NRG’s response to question 2 for additional detail.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

No. Please see NRG’s response to question 2 for additional detail.

Likes 0	
Dislikes 0	

Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Conforming changes to CIP-003 - CIP-013 are dependent on ambiguous definitions introduced in CIP-002 and CIP-005.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
Xcel Energy generally supports conforming changes to these standards. However, Xcel Energy does not agree with the proposed changes to the applicable systems column in these standards. Independly identified SCI is listed throughout the applicable systems column and with our concern with the lack of clarity in Independly identified SCI, we can not support at this time. While Xcel Energy does not support the approval of this Standard at this time, we do support other aspects in the modifications made as identified in EEI comments.	
Likes 0	
Dislikes 0	
Response	
Clarice Zellmer - WEC Energy Group, Inc. - 5	
Answer	No
Document Name	
Comment	
See MRO-NSRF and EEI Comments	
Likes 0	

Dislikes 0	

Response

Ronald Bender - Nebraska Public Power District - 5

Answer	No
Document Name	

Comment

We do not agree with the proposed changes to these Reliability Standards and do not believe these specific standards need revising.

The requirements in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 are more policy and process focused than the more technical requirements of CIP-005, CIP-007, and CIP-010. Thus, the requirements among the larger population of CIP standards should apply regardless of the technologies in use (ex. you are required to have a process for PRA, to have an Incident Response Plan, to have one or more recovery plans, etc.). Virtual assets or mixed-trust environments should not impact the requirements in these standards.

Second, the proposed change is only to include the phrase “SCI identified independently supporting an Applicable System.” As noted above this is a confusing phrase and not at all clear how an SCI could be both independent and supporting. These terms are incongruous when used together in the same phrase.

If there is concern that going forward some virtual assets may improperly be left out of the scope of CIP requirements, we note that the proposed revised definition of BES Cyber System would include “Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.” This should be sufficient to allow each Responsible Entity to identify its BES Cyber Systems including virtual technologies under CIP-002 and then comply with the requirements of CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 without the need for changing the Applicability Section of each Standard. [We also note the possibility that by including the phrase about Shared Cyber Infrastructure separate from BES Cyber System we are opening the door to compliance at the asset level instead of the system level, and thus undoing one of the improvements from the CIP v5/6 revisions.]

We recommend retracting the revisions for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013, and only moving forward with revisions to CIP-002, CIP-005, CIP-007, and CIP-010 to address virtual assets and mixed-trust environments.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Comments: Comments: For the CIP-013 Standard, we do not agree with the part 4.2.3 Exemptions, specially 4.2.3.3. How do you define “Cyber systems who provide confidentiality and integrity of an ESP that extends to one or more geographic locations” ?

Suggestion: 4.2.3.2 Cyber Systems *and Shared Cyber Infrastructure(SCI)* associated with communication links logically isolated from, providing *or not* logical isolation between discrete Electronic Security Perimeters (ESP).

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	

Comment

We do not agree with the proposed changes to these Reliability Standards and do not believe these specific standards need revising.

The requirements in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 are more policy and process focused than the more technical requirements of CIP-005, CIP-007, and CIP-010. Thus, the requirements among the larger population of CIP standards should apply regardless of the technologies in use (ex. you are required to have a process for PRA, to have an Incident Response Plan, to have one or more recovery plans, etc.). Virtual assets or mixed-trust environments should not impact the requirements in these standards.

Second, the proposed change is only to include the phrase “SCI identified independently supporting an Applicable System.” As noted above this is a confusing phrase and not at all clear how an SCI could be both independent and supporting. These terms are incongruous when used together in the same phrase.

If there is concern that going forward some virtual assets may improperly be left out of the scope of CIP requirements, we note that the proposed revised definition of BES Cyber System would include “Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.” This should be sufficient to allow each Responsible Entity to identify its BES Cyber Systems including virtual technologies under CIP-002 and then comply with the requirements of CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 without the need for changing the Applicability Section of each Standard. [We also note the possibility that by including the phrase about Shared Cyber Infrastructure separate from BES Cyber System we are opening the door to compliance at the asset level instead of the system level, and thus undoing one of the improvements from the CIP v5/6 revisions.]

We recommend retracting the revisions for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013, and only moving forward with revisions to CIP-002, CIP-005, CIP-007, and CIP-010 to address virtual assets and mixed-trust environments.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Several of the terms and their usage, especially SCI, lends ambiguity with their use in the Standards. Further clarifications and refinements of the terms should be given attention.

Likes 0	
Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	No
Document Name	

Comment

CIP-003: In requirement R2 refers to “SCI that supports any part of a low impact BCS” but the VSL for R2 only refers to “SCI” without stating “that supports any part of a low impact BCS.”

CIP-004: CEHE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-006: CEHE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-008: CEHE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-009: CEHE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-011: CEHE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-013: CEHE proposes to replace “SCI identified independently supporting these BCS or their associated EACMS and PACS.” with “independent SCI that supports these BCS or their associated EACMS and PACS.” In the VSLs for R1 and R2 it refers to “… BES Cyber Systems, and their associated EACMS, PACS, and SCI, …”, there are no descriptors around SCI, such as “independent SCI”.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA does not support the modified language. How SCI is to be independently identified is not clear.

Likes 0	
Dislikes 0	

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

CIP-003: In requirement R2 refers to “SCI that supports any part of a low impact BCS” but the VSL for R2 only refers to “SCI” without stating “that supports any part of a low impact BCS.”

CIP-004: SIGE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-006: SIGE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-008: SIGE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-009: SIGE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-011: SIGE proposes for the Applicable Systems column to replace, “SCI identified independently supporting an Applicable System above” with “Independent SCI that supports an Applicable System above.”

CIP-013: SIGE proposes to replace “SCI identified independently supporting these BCS or their associated EACMS and PACS.” with “independent SCI that supports these BCS or their associated EACMS and PACS.”   In the VSLs for R1 and R2 it refers to “… BES Cyber Systems, and their associated EACMS, PACS, and SCI, …”, there are no descriptors around SCI, such as “independent SCI”.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Joe Tarantino

Answer	No

Document Name	
Comment	
The last draft of the standard seemed clearer. It's not clear what the existing changes are solving.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
All of the standards (CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013) referred in this question are proposed with a change the phrase "SCI identified independently supporting an Applicable System." This phrase requires more clarity from the SDT team as to what is meant by an SCI being independent and as well as supporting an applicable system. The terms used here have some level of ambiguity specifically when used in conjunction with each other. SDT is requested to provide examples and better clarity on this phrase as it pertains and becomes applicable as a proposed change to all of the above listed standards. Secondly as advised in the comments above while the new and revised defined terms are seen by BC Hydro to accommodate virtualization and future technologies, BC Hydro does not agree with the 'as is' state of the SCI definition proposed in this project comment/ballot submission. As explained in the comments of Questions 10 related to CIP-005, Question 11 related to CIP-007 and Question 11 related to CIP-010 above BC Hydro does not agree with the changes in the NERC glossary of terms introduced in Draft 2 of Project 2016-02.	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Cogentrix Energy Power Management, LLC - 5	
Answer	No
Document Name	
Comment	
We support NPCC TFIST's comments as found below: For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs For CIP-011, see BCSI comment in Q8	

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013's use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – "EERC"

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

Likes 0	
Dislikes 0	

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer	No
Document Name	

Comment

OKGE supports EEI's comments.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	

Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

In support of NPCC RSC comments.

For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs

For CIP-011, see BCSI comment in Q8

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013's use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – "EERC"

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

It is difficult to agree with the revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 standards as there are too many questions and uncertainty surrounding the proposed changes.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

While AEP supports conforming formatting changes and removal of Background and Technical Rationale, we do still have concerns regarding some of the terms proposed to be added to Applicable Systems (as stated in the responses to Questions #1 through #8 above). We recommends adding clarification on “SCI identified independently”, as this phrase has been added to Applicable Systems column for many of the CIP standards. AEP recommends that the terms and definitions should be clarified before included in the standard revisions.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments 1:

We disagree with the changes in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.

Recommendations:

- Resulting from our proposed changes to the definitions (See our comments in Q1), we suggest removing SCI language from all Applicable Systems.

Comments 2:

We do not agree with the proposed changes to these Reliability Standards and do not believe these specific standards need revising.

The requirements in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 are more policy and process focused than the more technical requirements of CIP-005, CIP-007, and CIP-010. Thus, the requirements among the larger population of CIP standards should apply regardless of the technologies in use (ex. you are required to have a process for PRA, to have an Incident Response Plan, to have one or more recovery plans, etc.). Virtual assets or mixed-trust environments should not impact the requirements in these standards.

Second, the proposed change is only to include the phrase “SCI identified independently supporting an Applicable System.” As noted above this is a confusing phrase and not at all clear how an SCI could be both independent and supporting. These terms are incongruous when used together in the same phrase.

If there is concern that going forward some virtual assets may improperly be left out of the scope of CIP requirements, we note that the proposed revised definition of BES Cyber System would include “Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.” This should be sufficient to allow each Responsible Entity to identify its BES Cyber Systems including virtual technologies under CIP-002 and then comply with the requirements of CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 without the need for changing the Applicability Section of each Standard. [We also note the possibility that by including the phrase about Shared Cyber Infrastructure separate from BES Cyber System we are opening the door to compliance at the asset level instead of the system level, and thus undoing one of the improvements from the CIP v5/6 revisions.]

We recommend retracting the revisions for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013, and only moving forward with revisions to CIP-002, CIP-005, CIP-007, and CIP-010 to address virtual assets and mixed-trust environments.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs

For CIP-011, see BCSI comment in Q8

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013’s use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – “EERC”

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

It is difficult to agree with the revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 standards as there are too many questions and uncertainty surrounding the proposed changes.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster

Answer	No
Document Name	

Comment

Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Great River Energy - 3

Answer	No
Document Name	

Comment	
GRE agrees with the comments submitted by the NSRF.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC	
Answer	No
Document Name	
Comment	
In support of IRC SRC/SWG. For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs For CIP-011, see BCSI comment in Q8 Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2. Request clarification on CIP-013's use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013? Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version. Request correction of typo in CIP-006 R2.2 Applicability – "EERC" Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

The proposed changes to the above requirements (CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013), should not be revised, but be left as is.

Since these requirements are policy and process focused than the technical requirements of CIP-005, CIP-007 and CIP-010. In saying this (CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013) should apply regardless of technology.

Again the phrase “SCI identified independently supporting an Applicable System” The phrase is confusing and up to interparation.

We do not agree with the proposed changes to these Reliability Standards and do not believe these specific standards need revising.

The requirements in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 are more policy and process focused than the more technical requirements of CIP-005, CIP-007, and CIP-010. Thus, the requirements among the larger population of CIP standards should apply regardless of the technologies in use (ex. you are required to have a process for PRA, to have an Incident Response Plan, to have one or more recovery plans, etc.). Virtual assets or mixed-trust environments should not impact the requirements in these standards.

Second, the proposed change is only to include the phrase “SCI identified independently supporting an Applicable System.” As noted above this is a confusing phrase and not at all clear how an SCI could be both independent and supporting. These terms are incongruous when used together in the same phrase.

If there is concern that going forward some virtual assets may improperly be left out of the scope of CIP requirements, we note that the proposed revised definition of BES Cyber System would include “Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.” This should be sufficient to allow each Responsible Entity to identify its BES Cyber Systems including virtual technologies under CIP-002 and then comply with the requirements of CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 without the need for changing the Applicability Section of each Standard. [We also note the possibility that by including the phrase about Shared Cyber Infrastructure separate from BES Cyber System we are opening the door to compliance at the asset level instead of the system level, and thus undoing one of the improvements from the CIP v5/6 revisions.]

We recommend retracting the revisions for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013, and only moving forward with revisions to CIP-002, CIP-005, CIP-007, and CIP-010 to address virtual assets and mixed-trust environments.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

We do not support the proposed changes in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.

Recommendations:

- Resulting from our proposed changes to the definitions (See our comments in Q1), we suggest removing SCI language from all Applicable Systems.

The requirements in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 are more policy and process focused than the more technical requirements of CIP-005, CIP-007, and CIP-010. Thus, the requirements among the larger population of CIP standards should apply regardless of the technologies in use (ex. you are required to have a process for PRA, to have an Incident Response Plan, to have one or more recovery plans, etc.). Virtual assets or mixed-trust environments should not impact the requirements in these standards.

Second, the proposed change is only to include the phrase "SCI identified independently supporting an Applicable System." As noted above this is a confusing phrase and not at all clear how an SCI could be both independent and supporting. These terms are incongruous when used together in the same phrase.

If there is concern that going forward some virtual assets may improperly be left out of the scope of CIP requirements, we note that the proposed revised definition of BES Cyber System would include "Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports." This should be sufficient to allow each Responsible Entity to identify its BES Cyber Systems including virtual technologies under CIP-002 and then comply with the requirements of CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 without the need for changing the Applicability Section of each Standard. [We also note the possibility that by including the phrase about Shared Cyber Infrastructure separate from BES Cyber System we are opening the door to compliance at the asset level instead of the system level, and thus undoing one of the improvements from the CIP v5/6 revisions.]

We recommend retracting the revisions for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013, and only moving forward with revisions to CIP-002, CIP-005, CIP-007, and CIP-010 to address virtual assets and mixed-trust environments.

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	No
Document Name	
Comment	
CIP-003 Requirement 2/Attachment 1 appear to either be in conflict or redundant to CIP-010 R4 where the language "except for use on low impact BCS or SCI supporting only low impact BCS(s)". The actual requirements for TCA for Low BCS are ambiguous given this redundancy or conflict.	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	No
Document Name	
Comment	

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan

Answer	No
Document Name	

Comment
OPG concurs with NPCC's RSC comments

Likes 0	
Dislikes 0	

Response
Becky Webb - Exelon - 6

Answer	No
Document Name	

Comment
Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response
Christopher McKinnon - Eversource Energy - 3, Group Name Eversource 1

Answer	No
Document Name	

Comment
For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs

For CIP-011, see BCSI comment in Q8

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013's use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – "EERC"

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

Likes 0

Dislikes 0

Response

Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE

Answer	No
Document Name	

Comment

<duplicate>

Likes 0

Dislikes 0

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT supports the IRC SRC comments.

Likes 0

Dislikes 0

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI supports the changes made to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011 and CIP-013 except as described below:

- CIP-003: EEI supports the proposed conforming changes but proposes the following for Attachment 1 Section 5, 5.1 and 5.2.

  “Controls that maintain the state of the operating system and software such that it is in a known state prior to use;”.

- CIP-004: The phrase “SCI identified independently” is frequently used throughout CIP-004 but is unclear in its intent and needs to be clarified before EEI can support the revisions to this Reliability Standard.
- CIP-006: The phrase “SCI identified independently” is frequently used throughout CIP-006 but is unclear in its intent and needs to be clarified before EEI can support the revisions to this Reliability Standard. The following concerns should also be addressed:

1) *Requirement R1, Subpart R1.10 was removed and the technical rationale states that the requirements were fully moved to CIP-005, Subpart 1.4 but their associated PCAs were not included, which represents an unintentional reliability gap.*

2) EEI notes that within the Applicable Systems column of Part 1.1, the term “hosting” is used in “SCI without ERC hosting Medium Impact BCS”, but “hosting” has been changed to “supporting” in other places.

- CIP-008: The phrase “SCI identified independently” is frequently used throughout CIP-008 but is unclear in its intent and needs to be clarified before EEI can support the revisions to this Reliability Standard.
- CIP-009: The phrase “SCI identified independently” is unclear. Additionally, restoration plans as currently described are too prescriptive and should not be tied to the restoration of SCI even if an entity intends to utilize virtualization. The focus should be the restoration of critical systems necessary for restoration and not predefine how entities define their restoration plans. For example, an entity may decide to incorporate into their restoration plan a more barebones approach that restores an image to a dedicated server without the restoration of SCI. While this may not restore their systems in an identical fashion to what they were operating prior to the failure, it would allow them to quickly and efficiently restore their critical systems. The objective of a recovery plan should focus on the recovery of those critical systems (i.e., BCS, EACMS and PACS functionality). For those entities who chose to take another approach such as restore their SCI as a part of their recovery plan, they too would not be limited by this Reliability Standard. Such an approach would provide flexibility and promote a results-based approach.

Applicable Systems column of Parts 2.1 and 2.2, the term “hosting” is used in “SCI hosting Medium Impact BCS at Control Centers or their …”, but “hosting” has been changed to “supporting” in other places. This difference should either be explained or corrected if it was an unintentional error.

- CIP-011: The phrase “SCI identified independently” is used throughout CIP-011 but is unclear in its intent and needs to be clarified before EEI can support the revisions to this Reliability Standard. .
- CIP-013: The phrase “SCI identified independently” is used in Requirement R1 of CIP-013 but is unclear in its intent and needs to be clarified before EEI can support the revisions to this Reliability Standard.

Likes 0

Dislikes 0

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis	
Answer	No
Document Name	
Comment	
PJM signs on to the comments provided by the IRC SRC.	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
John Liang - Snohomish County PUD No. 1 - 6	
Answer	No
Document Name	
Comment	
SNPD supports the comments provided by Sacramento Municipal Utility District (SMUD).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No

Document Name	

Comment

For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs

For CIP-011, see BCSI comment in Q8

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013's use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – "EERC"

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

It is difficult to agree with the revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 standards as there are too many questions and uncertainty surrounding the proposed changes.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	No
Document Name	

Comment

For CIP-003 Attachment 1 Section 5, see Q12 comments on TCAs

For CIP-011, see BCSI comment in Q8

Suggest moving CIP-011 R2 to CIP-002 so the entire BCS lifecycle question is one Standard. Also suggest expanding this disposal and reuse language beyond BCSI. We believe the BCSI SDT could not recommend this change because it was not in their SAR. There is potential double jeopardy between the proposed CIP-011 R2 and CIP-011 R1.2.

Request clarification on CIP-013’s use of high and medium impact. This Standard uses upper and lower case. Other Standards use capitalization. Is there a difference? If so, please explain

Request clarification on CIP-013 before the Requirements section. Were the conforming changes in the other CIP Standards made in this earlier part of CIP-013?

Request clarification on CIP-013 R1. Are these updates conforming changes OR expansion of scope? It is hard to tell without a redline to the last approved version.

Request correction of typo in CIP-006 R2.2 Applicability – “EERC”

Request clarification of SCI supporting multiple Impact Ratings. Is this scenario double or triple jeopardy?

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	No
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Nurul Abser - NB Power Corporation - 1

Answer	No
Document Name	

Comment

With respect to CIP-011 changes, R.1.2. and R.2.1. appear to be the same requirement. We suggest incorporating the measure for R2.1 into R1.2 and eliminating R.2.1.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD

Answer	Yes
Document Name	

Comment

Chelan agrees with the conforming changes.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	Yes
Document Name	

Comment

CIP-003:

Section 3.1 - suggest removing ‘as determined by the Responsible Entity’ as it is already stated in Attachment 1.

Section 3.1, second bullet – Change ‘an SCI’ to just SCI

Section 3.1, Should ‘and a system(s) outside:’ be changed to ‘and a Cyber System outside:’

CIP-004, Part 2.1.9 – Would the intended scope be more accurate by changing Cyber Systems to CIP Systems?

Cyber security risks associated with electronic interconnectivity and interoperability with other CIP Systems, including Transient Cyber Assets, and with Removable Media.

CIP-013, R1.1 and R1.2 – Would the scope more accurately be identified by changing ‘system’ to ‘CIP Systems?’

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed conforming changes to the Reliability Standards, *except* for the following: CIP-006 R1.10 is not fully covered by CIP-005 R1.4 as it leaves the associated PCAs unaccounted for.

Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
ACES supports the changes and does not believe the inclusion of “SCI identified independently…” in these standards increase compliance burden and are used for clarification of what is included in the Applicable Systems. Our opinion is predicated on clarifying “SCI identified independently…” as noted in question #2. AEPC signed on to ACES comments.	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
SDG&E supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power	

Answer	Yes
Document Name	
Comment	
MEAG Power adopts the Southern Company comments.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3	
Answer	Yes
Document Name	
Comment	
We agree with the conforming changes. However, please correct the CIP-003 exemption to be consistent with the other standards.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	

Answer	Yes
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	Yes
Document Name	

Comment

We agree with the confroming changes. However, please correct the CIP-003 exemption to be consistent with the other standards.

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; John Merrell, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Marc Donaldson, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 3, 1, 4, 5, 6; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Tacoma Power agrees with the proposed changes to the NERC Glossary terms. However, we identified the following improvements and minor corrections to the CIP-003 and CIP-006 documentation:

- CIP-003 Attachment 1 Section 1 has inconsistent language for the inclusion of SCI. Suggest modifying to “...SCI that supports any part of a low impact BCS...”
- CIP-009 R2.1 and R2.2, the redline should delete the following item from the Applicable System column: “SCI hosting High or Medium Impact BCS at Control Centers or their associated: • PACS; or • EACMS”

Likes 0	
Dislikes 0	

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer	Yes
Document Name	

Comment

We agree with the conforming changes. However, please correct the CIP-003 exemption to be consistent with the other standards.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

Relative to CIP-003, the inclusion of a reference to SCI in R2, which addresses low impact assets, would seem to suport the inclusion of SCI where SCI is independently identified, but supporting a high or medium impact BCS. However, this language was struck from the requirement despite the fact that independently identified BCS supporting an applicable system is subject to several requirements and standards addressed within the policies required under R1. Further, this raises a question as to whether SCI grouped with BCS would be subject to CIP-003 by virtue of their grouping while independently identified SCI would not. For this reason, GSOC requests clarification regarding whether SCI that is identified independent of BCS, but is supporting such systems should be addressed in the policies required under CIP-003, R1.

Relative to CIP-005, GSOC recommends revising the following language

Real-time Assessment and Realtime monitoring data while being transmitted between Control Centers subject to CIP012; and

as follows:

Real-time Assessment and Realtime monitoring data subject to CIP012; and.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations

Answer	Yes

Document Name	
Comment	
ACES supports the changes and does not believe the inclusion of “SCI identified independently…” in these standards increase compliance burden and are used for clarification of what is included in the Applicable Systems. Our opinion is predicated on clarifying “SCI identified independently…” as noted in question #2.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
For CIP-006 R1.1, Southern believes the first "SCI without ERC hosting Medium Impact BCS" is unnecessary and we suggest deletion. For CIP-009, we suggest deleting "SCI identified independently" throughout the standard. The goal of CIP-009 according to R1.3 and the GTB is to recover the functionality of the BCS. In the "all-in" scenario, the SCI underlay isn't called out as a specific component of a recovery plan. To recover the functionality of a system, such as a virtualized EACMS, the entity may restore an image to a dedicated server HW without SCI. The SCI should not be a specific object of recovery plans - the object is to recover the BCS, EACMS, or PACS functionality. If recovery of the SCI is required by the entity to recover the BCS functionality, that would be required as part of the plan but not a distinct object of the requirement. If SCI applicability is left in CIP-009, it seems duplicated throughout most of R2's requirement parts. The edits made in R1 and R3 to applicable systems were not made in R2. The 'applicable system' in R2.2 should be capitalized. R2.2 and in particular its measures need to be updated for virtualization scenarios. It maintains a sense of tape backups of static files.	
Likes 0	

Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
We agree with the conforming changes. However, please correct the CIP-003 exemption to be consistent with the other standards.	
Likes 0	
Dislikes 0	
Response	
Ryan Olson - Portland General Electric Co. - 5	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	
Dan Zollner - Portland General Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Portland General Electric Company supports this change, but generally agrees with the comments provided by EEI for this survey question.	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Susan Sosbe - Wabash Valley Power Association - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Jones - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

14. Please provide any additional comments for the SAR drafting team to consider, if desired.

Daniel Mason - Portland General Electric Co. - 6, Group Name PGE FCD

Answer

Document Name

Comment

Portland General Electric Company is providing the following comments for the drafting team's consideration:

CIP-005-8 R2.6.2 – “Applicable Systerms” is used instead of “Applicable Systems”

CIP-005-8 R2.1 - In the Applicable Systems column, the phrase "Intermediate Systems used to access Applicable Systems of Part 2.1" is included. However, the requirement states that Responsible Entities must "Permit authorized IRA, if any, only through an Intermediate System." Portland General Electric Company believes this implies that an Intermediate System would need to broker access to the Intermediate System that is brokering access to the other Applicable Systems in R2.1. Portland General Electric Company wonders if it was the drafting team’s intent to include "Intermediate Systems used to access Applicable Systems of Part 2.1."

Likes 0

Dislikes 0

Response

Dan Zollner - Portland General Electric Co. - 3

Answer

Document Name

Comment

Portland General Electric Company is providing the following comments for the drafting team's consideration:

CIP-005-8 R2.6.2 – “Applicable Systerms” is used instead of “Applicable Systems”

CIP-005-8 R2.1 - In the Applicable Systems column, the phrase "Intermediate Systems used to access Applicable Systems of Part 2.1" is included. However, the requirement states that Responsible Entities must "Permit authorized IRA, if any, only through an Intermediate System." Portland General Electric Company believes this implies that an Intermediate System would need to broker access to the Intermediate System that is brokering access to the other Applicable Systems in R2.1. Portland General Electric Company wonders if it was the drafting team’s intent to include "Intermediate Systems used to access Applicable Systems of Part 2.1."

CIP-006-7 R1.6 - In the Applicable Systems column, there should be a bullet next to "Medium Impact BCS with ERC" so that the Applicable Systems column reads "Physical Access Control Systems (PACS) associated with: • High Impact BCS, or • Medium Impact BCS with ERC"

CIP-006-7 R1.6 - The requirement language says, "Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System." However, SCI identified independently is only supporting PACS, not categorized as part of the PACS itself. For clarity, Portland General Electric Company suggest rephrasing the requirement language to say, "Monitor Applicable Systems for unauthorized physical access."

CIP-006-7 R1.7 - The requirement language says, "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection." However, SCI identified independently is only supporting PACS, not categorized as part of the PACS itself. For clarity, Portland General Electric Company suggest rephrasing the requirement language to say, "Issue an alarm or alert in response to detected unauthorized physical access to an Applicable System to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection."

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	
Document Name	

Comment

ITC supports the response submitted by EEI for this question.

Likes 0	
Dislikes 0	

Response

Bobbi Welch - Midcontinent ISO, Inc. - 2, Group Name ISO/RTO Council Standards Review Committee 2016-02 Virtualization (Draft 2)

Answer	
Document Name	

Comment

Overall, the ISO/RTO Council (IRC) Standards Review Committee (SRC)[1] recommends a separate virtualization standard be adopted to reduce the amount of change, additional work and confusion that will be required by a more holistic change as noted by the SDT. The new standard should be limited to only the requirements that directly relate to virtualization technology (e.g. dedicated infrastructure, shared infrastructure and management systems). In the event the SDT declines to pursue a separate virtualization standard, the SRC offers these comments in Questions 1-14 on the draft standards as presented.

Are these comments for the SAR drafting team or the Standards drafting team per the question’s text?

Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries.

Request that the SDT post the draft revisions as “red-line to last approved” rather than “to last posted.” This expectation is consistent with posting of other NERC Standards and earlier postings of CIP updates.

Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?

[1] For purposes of these comments, the IRC SRC includes the following entities: CAISO, ERCOT, IESO, ISO-NE, MISO, NYISO, SPP and PJM (with the exception of our response to question 14, paragraph 1).

Likes 0

Dislikes 0

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer

Document Name

Comment

N&ST believes the proposed “Exemption” statement in every CIP Standard, 4.2.3.3, “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an Electronic Security Perimeter (ESP) that extends to one or more geographic locations” is both confusing and inaccurate. One provides for the confidentiality and integrity of data, not ESPs. N&ST suggests rewording that’s consistent with the language of proposed CIP-005 Requirement R1 Part 1.4, such as “Cyber Systems associated with communication links used to span a single ESP among two or more geographic locations.”

N&ST reviewed proposed VSL revisions only briefly, but noticed the High and Severe VSLs for CIP-005 Requirement R1 still refer to Requirement Parts (1.2.1 through 1.2.3) that the SDT has deleted. N&ST recommends a thorough proofreading of all VSLs to ensure they reflect the latest proposed Requirement changes.

Likes 0

Dislikes 0

Response

Ryan Olson - Portland General Electric Co. - 5

Answer

Document Name

Comment

Portland General Electric Company is providing the following comments for the drafting team's consideration:

CIP-005-8 R2.6.2 – “Applicable Syste[r]ms” is used instead of “Applicable Systems”

CIP-005-8 R2.1 - In the Applicable Systems column, the phrase "Intermediate Systems used to access Applicable Systems of Part 2.1" is included. However, the requirement states that Responsible Entities must "Permit authorized IRA, if any, only through an Intermediate System." Portland General Electric Company believes this implies that an Intermediate System would need to broker access to the Intermediate System that is brokering access to the other Applicable Systems in R2.1. Portland General Electric Company wonders if it was the drafting team's intent to include "Intermediate Systems used to access Applicable Systems of Part 2.1."

CIP-006-7 R1.6 - In the Applicable Systems column, there should be a bullet next to "Medium Impact BCS with ERC" so that the Applicable Systems column reads "Physical Access Control Systems (PACS) associated with: • High Impact BCS, or • Medium Impact BCS with ERC"

CIP-006-7 R1.6 - The requirement language says, "Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System." However, SCI identified independently is only supporting PACS, not categorized as part of the PACS itself. For clarity, Portland General Electric Company suggest rephrasing the requirement language to say, "Monitor Applicable Systems for unauthorized physical access."

CIP-006-7 R1.7 - The requirement language says, "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection." However, SCI identified independently is only supporting PACS, not categorized as part of the PACS itself. For clarity, Portland General Electric Company suggest rephrasing the requirement language to say, "Issue an alarm or alert in response to detected unauthorized physical access to an Applicable System to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection."

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	
Document Name	

Comment

Are these comments for the SAR drafting team or the Standards drafting team per the question's text?

Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries

Request that the SDT post the draft revisions as "red-line to last approved" rather than "to last posted." This expectation is consistent with the posting of other NERC Standards and earlier postings of CIP updates.

Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?

Likes 0	
Dislikes 0	

Response

John Liang - Snohomish County PUD No. 1 - 6

Answer

Document Name

Comment

The term “SCI” is mentioned several times in the draft document, but it is not being spelled out exactly what it is.

Associated Data Center (as required by the latest ERT v5 spreadsheet) is not listed in the draft standard.

Likes 0

Dislikes 0

Response

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer

Document Name

Comment

The term “SCI” is mentioned several times in the draft document, but it is not being spelled out exactly what it is.

Associated Data Center (as required by the latest ERT v5 spreadsheet) is not listed in the draft standard.

Likes 0

Dislikes 0

Response

Holly Chaney - Snohomish County PUD No. 1 - 3, Group Name SNPD Voting Members

Answer

Document Name

Comment

The term “SCI” is mentioned several times in the draft document, but it is not being spelled out exactly what it is.

Associated Data Center (as required by the latest ERT v5 spreadsheet) is not listed in the draft standard.

Likes 0

Dislikes 0

Response

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5

Answer	
Document Name	

Comment

The term “SCI” is mentioned several times in the draft document, but it is not being spelled out exactly what it is.

Associated Data Center (as required by the latest ERT v5 spreadsheet) is not listed in the draft standard.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

Planned and Unplanned changes language should be added to the Implementation Plan, similar to the language included in previous CIP implementation plans. *(See Implementation Plan For Version 5 CIP Cyber Security Standards, November 7, 2011; Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012; and Implementation Plan - Project 2014-02 CIP Version 5 Revisions, January 23, 2015.)*

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - Elizabeth Davis On Behalf of: Tom Foster, PJM Interconnection, L.L.C., 2; - Elizabeth Davis

Answer	
Document Name	

Comment

PJM appreciates and supports the continued work of the Standards Drafting Team (SDT) to transition the framework of the NERC CIP standards to one that more readily supports the use of virtualization technology. While PJM recognizes the significant challenges associated with developing revisions and building consensus within the industry, we believe it is critical to sustain the current momentum and finalize these changes. These changes are important not only to better enable the use of virtualization technology to support the reliability of BES Cyber Systems, but also – and more importantly - to better enable the industry’s use of emerging technologies in the future. PJM believes the SDT’s work to update the standards framework will position the industry to take earlier advantage of new technologies to increase reliability as the revised standards will be based more on controls rather than technology type. While there is the possibility that changes to the standards could still result from the introduction of new technologies, these changes should be minimal if the framework of the standards is based on controls.

Likes 0

Dislikes 0

Response

Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1

Answer

Document Name

Comment

The term “SCI” is mentioned several times in the draft document, but it is not being spelled out exactly what it is.

Associated Data Center (as required by the latest ERT v5 spreadsheet) is not listed in the draft standard.

Likes 0

Dislikes 0

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer

Document Name

Comment

1) Planned and Unplanned changes language is missing in this version’s implementation plan, and this should be included.

2) Although EEI is not permitted to ballot on these proposed changes to the CIP Reliability Standards, we note that Industry was not afforded an opportunity to vote on the proposed changes to the New, Modified and Retired NERC Glossary of Terms. Section 5.0 of the Standard Processes Manual states that “Glossary of Terms includes terms that have been through the **formal approval process**”, which EEI understands to mean that new terms are to be balloted. Therefore, the proposed terms that have been modified, added, or retired will need to be balloted prior to the final approval of the proposed CIP Reliability Standards.

3) EEI notes that acronym for Shared Cyber Infrastructure (SCI) is used prominently in many of the proposed new NERC CIP Standards but is often not identified in its first use in the following Reliability Standards. (See below)

CIP-002-7 – SCI used 27 times but never identified as Shared Cyber Infrastructure
CIP-004-Y - SCI is used 23 times but never identified as Shared Cyber Infrastructure
CIP-005-8 – SCI is used 30 times but never identified as Shared Cyber Infrastructure
CIP-006-7 - SCI is used 17 times but never identified as Shared Cyber Infrastructure
CIP-007-7 – SCI is used 23 times but never identified as Shared Cyber Infrastructure
CIP-008-7 – SCI is used 12 times but never identified as Shared Cyber Infrastructure

CIP-009-7 – SCI is used 12 times but never identified as Shared Cyber infrastructure
CIP-010-5 – SCI is used 15 times but never identified as Shared Cyber infrastructure
CIP-011-Y – SCI is used 3 times but never identified as Shared Cyber infrastructure
CIP-013-3 – SCI is used 17 times but never identified as Shared Cyber infrastructure

Likes 0	
Dislikes 0	

Response

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6

Answer	
Document Name	

Comment

Recommend spelling out "Shared Cyber Infrastructure" within CIP-002 standard text

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	
Document Name	

Comment

ERCOT supports the IRC SRC comments and offers these additional comments:

- Redlines to the current approved standard would be appreciated to understand the changes between current obligations and the proposed changes.
- Due to the differences in traditional and virtual technologies, the SDT should consider moving the virtual requirements to a separate standard or standards. This will reduce confusion when applying the requirements and allow those who do not plan to use virtualization to focus on the requirements relevant to them and not be distracted by terminology and requirements that do not apply to them.
- BES Cyber System definition: The proposed definition appears to require two separate groupings if SCI is in use, one for the BES Cyber Assets, and one for the Shared Cyber Infrastructure. Recommend a simplification, "One or more BES Cyber Assets logically grouped by a Responsible Entity to perform one or more reliability tasks for a functional entity, and the Shared Cyber Infrastructure supporting the BES Cyber Assets supported."

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment

As pertaining to EACMS and with the broadening and nesting of definitions, the need for the EACS/EAMS split becomes more evident, and possibly even different types of EACS (or no type at all) as it appears the requirements are trying to specify requirements for firewalls as opposed to domain controllers as one example. As Zero Trust, policy enforcement within hypervisors, virtual FW's, etc. proliferate, the broad definition of EACMS as a “thing” is becoming more of an issue with virtualization. Electronic Access Control is a function and not a type of CA or VCA and virtualization and zero trust are making this ever more evident. Including logging systems that only monitor access in the same definition adds to the issue. The standards appear to begin to split this broad category with phrases like "EACMS that enforce an ESP", but that is also problematic. Domain Controllers (DC) 'enforce a policy' that can 'control communications', yet some of the requirements that use this scope can’t be applied to a DC. (CIP-005 R1.2 and R1.3 for example. R1.3 would break most systems as it could require that a virtual BCS can't talk to a DC. Although we understand the intent is to prevent virtual tenant access to the SCI management plane, it says far more due to the intertwining of definitions. This requirement says a virtual BCS on independent SCI must be prevented from communications to the Management Interface, which is defined as "a user interface that is…used to configure an ESP" which is defined as "…policies enforced by an EACMS that controls communications". The virtual BCS cannot communicate to the Domain Controller (breaking the BCS) because the DC may enforce group policy that may control communications (what ports or services are enabled/disabled on servers). Attempting to do electronic access control to an EACMS management plane is perilous with these broad constructs. "Electronic access control" is a broad function with no differentiation between IP network type access control (firewalls) and user/process authentication (domain controllers) or IRA access control (Intermediate Systems) or merely logging systems attempting to correlate events for detection. With the philosophy that every Cyber Asset or VCA is every definition it meets, this is an issue that needs simplification.

Regarding the Implementation Plan, it is missing the "Planned or Unplanned Changes Resulting in a Higher Categorization" section that should be included in order to carry that forward to the new version of CIP-002. The list of definitions in the Implementation Plan needs to be updated as well.

Likes 0	
Dislikes 0	

Response	
Maggy Powell - Amazon Web Services - 7	
Answer	
Document Name	
Comment	
The SDT has been clear that this project focuses on on-premise virtualization, however, many virtualization concepts could be interpreted as being related to cloud computing technologies. AWS suggests explicitly stating that the Standards do not apply to cloud within the Applicability section of CIP-002. If these updated Standards do not apply to cloud, it should be obvious to the reader. Thank you to the drafting team for all your work.	
Likes 0	
Dislikes 0	
Response	
Dana Showalter - Electric Reliability Council of Texas, Inc. - 2 - Texas RE	
Answer	
Document Name	
Comment	
<duplicate>	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Standard Collaborations	
Answer	
Document Name	
Comment	
Although ACES answered no to question #7, an ACES member agrees with the SDT in question #7, stating they see advantages to leveraging policies in zero trust environments to reduce overall burden of documenting ESPs. Further, they feel the differences in technology between traditional perimeter controls and zero trust would not hinder the audit process.	

We would like to thank the SDT for their hard work on this project and addressing industry comments. This draft is significantly closer to the existing standards while allowing the flexibility to incorporate newer and future technologies to protect the BES.	
Likes 0	
Dislikes 0	
Response	
Becky Webb - Exelon - 6	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
David Kwan - David Kwan On Behalf of: Constantin Chitescu, Ontario Power Generation Inc., 5; - David Kwan	
Answer	
Document Name	
Comment	
OPG concurs with NPCC's RSC comments	
Likes 0	
Dislikes 0	
Response	
Cynthia Lee - Exelon - 5	
Answer	
Document Name	
Comment	
Exelon is aligning with EEI in response to this question.	

Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	
Document Name	NEE-20210819-Virtualization_Unofficial_Comment_Form_06302021.pdf
Comment	
- The SDT has provided significant improvements in the July release yet a few clarifications are still required. We appreciate the efforts of SDT and supporting contributors. - Of the two following examples, which diagram, if the proposed definition change of ERC is accepted, depicts the ESP network of a typical substation? (see attached)	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
While GSOC understands the need for the standards and supporting technical rationale to comport to the new style and standards instituted by NERC and the contraints of format revisions, the loss of context in moving historical technical rationale supporting the standards to	

'retired' status creates ambiguity. Specifically, the movement of this substantive guidance to a retired section raises questions regarding whether portions of the guidance that remain applicable and are not clearly superseded can be relied upon by industry. For theses reasons, GSOC recommends that clarification be provided regarding whether substantive guidance provided in previous versions of the technical rationale that were moved to the 'retired' section in the latest version of the technical rationale and are not clearly superseded in the substantive portions of the new/revised technical rationale remain in effect and can be relied upon and utilized by industry in their compliance efforts. This clarification is critical because the movement of substantive guidance without replacement or clear superseding information reduces the overall guidance available to entities trying to adhere to a complex set of obligations.

GSOC appreciates the SDT's efforts on these changes. The proposed revisions are a substantive improvement and should address the majority of concerns previously expressed. Overall, GSOC supports the concepts proposed in the draft revisions.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	
Document Name	

Comment

We understand the SDT desires to allow flexibility for entity's to address a mixed trust environment, however the mixed trust environment may not be allowable based on our comments in Q1. In SDT proposed "independently Identified SCI" scenario (see the diagram in Q1), if the right side SCI containing a CIP Management Interface can remove a CIP cyber asset, the SCI should be identified as a CIP cyber asset (see our comments in Q1) resulting in all non-CIP VCAs it host becoming at least PCAs based on the affinity rule, therefore the proposed mixed trust model is broken and cannot provide flexibility for entities to achieve CIP compliance. To make the right side SCI out of CIP scope, the only way to do so is that the right side SCI cannot have a CIP Management Interface and its hosted VCAs cannot be CIP cyber assets. The only mixed trust environment can be done is the storage array. In our proposed changes, the storage array should be identified as part of the CIP cyber asset only if it contains the information for the real-time operation of a CIP cyber asset like a local hard drive and the rest of the storage array for storing historical information and non-real time information may be identified as a BCSI repository.

Entity's who choose to host both CIP and non-CIP cyber assets on SCI must understand the high security risk to the reliable operation of BES as changes to this complex environment could cause a misconfiguration, loss of service, security vulnerability or other issue which can impact the entire SCI virtual hardware platform and the hosts, VMs and their configurations. Also, resulting from our comments above, the non-CIP cyber assets on the mixed trust SCI becomes PCAs if the SCI contains CIP Management Interface in which it would bring additional compliance obligations to the Entity's who choose to do so.

Resulting from our proposed changes, the We believe the existing standard requirements and definitions could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, and reduce the impact to entity's existing CIP programs.

that affect the reliable operation of BES and provide greater clarity to auditors.

Likes 0

Dislikes 0

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer

Document Name

Comment

We concur with the SDT’s goal of revising the CIP standards to address virtualization, provide more options for Responsible Entities to remain compliant and ensure reliability while utilizing new and different technologies, and be objective-focused. To that end, we applaud the SDT’s continued work and effort on this project. While there are several negative comments listed above, we also feel that CIP-002, 005, 007, and 010 are also close to an acceptable revised state.

While the proposed revisions are made with the intent of allowing Responsible Entities more options to achieve compliance, the inclusion of multiple new and revised terms and requirement language across all CIP requirements gives the appearance of more complexity and thus more difficulty in achieving compliance. This may (or may not) only be an issue of optics but optics are important. The goal of providing Responsible Entities more options for compliance must not also detract from the goal of ensuring that the requirements are understandable and explainable to a wide audience.

The biggest concerns with all of these changes are:

CIP-002 – How will we identify if assets are in scope with the changes made to attachment 1

CIP-010 – How the removal of baseline configurations will affect SRP-PAC

We thank the SDT for this opportunity to provide comment and feedback.

Likes 0

Dislikes 0

Response

Casey Jones - Casey Jones On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Casey Jones

Answer

Document Name

Comment

Planned and Unplanned changes language should be added to the Implementation Plan, similar to the language included in previous CIP implementation plans. *(See Implementation Plan For Version 5 CIP Cyber Security Standards, November 7, 2011; Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012; and Implementation Plan - Project 2014-02 CIP Version 5 Revisions, January 23, 2015.)*

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC

Answer

Document Name

Comment

In support of IRC SRC/SWG.

Overall, the SRC recommends a separate virtualization standard be adopted to reduce the amount of change, additional work and confusion that will be required by a more holistic change as noted by the SDT. The new standard should be limited to only the requirements that directly relate to virtualization technology (e.g. dedicated infrastructure, shared infrastructure and management systems). In the event the SDT declines to pursue a separate virtualization standard, the SRC offers these comments in Questions 1-14 on the draft standards as presented.

Are these comments for the SAR drafting team or the Standards drafting team per the question’s text?

Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries request that the SDT post the draft revisions as “red-line to last approved” rather than “to last posted.” This expectation is consistent with posting of other NERC Standards and earlier postings of CIP updates.

Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?

Likes 0

Dislikes 0

Response

Michael Brytowski - Great River Energy - 3

Answer

Document Name

Comment

GRE agrees with the comments submitted by the NSRF.

Likes 0

Dislikes 0

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	
Document Name	

Comment

Planned and Unplanned changes language should be added to the Implementation Plan, similar to the language included in previous CIP implementation plans. *(See Implementation Plan For Version 5 CIP Cyber Security Standards, November 7, 2011; Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012; and Implementation Plan - Project 2014-02 CIP Version 5 Revisions, January 23, 2015.)*

Likes 0	
Dislikes 0	

Response

Amy Bratkovic - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	
Document Name	

Comment

Regarding new definitions, such as Cyber System and CIP System, the we requests an example collection that would meet each definition. Intermediate System? SIEM? A Venn diagram may also be useful.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	
Document Name	
Comment	
Evergy incorporates by reference and endorses the comments as filed by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Are these comments for the SAR drafting team or the Standards drafting team per the question's text? Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries Request that the SDT post the draft revisions as "red-line to last approved" rather than "to last posted." This expectation is consistent with posting of other NERC Standards and earlier postings of CIP updates. Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	

Comment

We understand the SDT desires to allow flexibility for entity’s to address a mixed trust environment, however the mixed trust environment may not be allowable based on our comments in Q1. In SDT proposed “independently Identified SCI” scenario (see the diagram in Q1), if the right side SCI containing a CIP Management Interface can remove a CIP cyber asset, the SCI should be identified as a CIP cyber asset (see our comments in Q1) resulting in all non-CIP VCAs it host becoming at least PCAs based on the affinity rule, therefore the proposed mixed trust model is broken and cannot provide flexibility for entities to achieve CIP compliance. To make the right side SCI out of CIP scope, the only way to do so is that the right side SCI cannot have a CIP Management Interface and its hosted VCAs cannot be CIP cyber assets. The only mixed trust environment can be done is the storage array. In our proposed changes, the storage array should be identified as part of the CIP cyber asset only if it contains the information for the real-time operation of a CIP cyber asset like a local hard drive and the rest of the storage array for storing historical information and non-real time information may be identified as a BCSI repository.

Entity’s who choose to host both CIP and non-CIP cyber assets on SCI must understand the high security risk to the reliable operation of BES as changes to this complex environment could cause a misconfiguration, loss of service, security vulnerability or other issue which can impact the entire SCI virtual hardware platform and the hosts, VMs and their configurations. Also, resulting from our comments above, the non-CIP cyber assets on the mixed trust SCI becomes PCAs if the SCI contains CIP Management Interface in which it would bring additional compliance obligations to the Entity’s who choose to do so.

Resulting from our proposed changes, the MRO NSRF believes the existing standard requirements and definitions could be revised more efficiently to meet the SAR requirements, ensure the virtualization security objectives are met, and reduce the impact to entity’s existing CIP programs. that affect the reliable operation of BES and provide greater clarity to auditors.

We thank the SDT for this opportunity to provide comment and feedback.

We concur with the SDT’s goal of revising the CIP standards to address virtualization, provide more options for Responsible Entities to remain compliant and ensure reliability while utilizing new and different technologies, and be objective-focused. To that end, we applaud the SDT’s continued work and effort on this project. While there are several negative comments listed above, we also feel that CIP-002, 005, 007, and 010 are also close to an acceptable revised state.

While the proposed revisions are made with the intent of allowing Responsible Entities more options to achieve compliance, the inclusion of multiple new and revised terms and requirement language across all CIP requirements gives the appearance of more complexity and thus more difficulty in achieving compliance. This may (or may not) only be an issue of optics but optics are important. The goal of providing Responsible Entities more options for compliance must not also detract from the goal of ensuring that the requirements are understandable and explainable to a wide audience.

We thank the SDT for this opportunity to provide comment and feedback.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	
Document Name	

Comment

While AEP has provided specific commentary on Questions 1 through 13, we would like to provide the following general thoughts as revisions are incorporated.

We ask the SDT to avoid, wherever possible, the nesting of defined terms within the definition of other defined terms. The current practice of nesting has made it difficult to support some of the great work that has already been put in by the SDT.

AEP recommends clarifying the definitions first, then firming up CIP-002 asset classification requirements in relation to the new definitions, so that the Standards conforming to these changes can be effectively implemented.

AEP anticipates that the outcome of this revision to the CIP standards to have significant impact on the manner by which Access Management and other tasks are performed. For example, this will require the development of controls in the areas of electronic access authorizations, reviews, revocations etc., related to BCSInfo on SCI. As such, we suggest SDT provides clarifications on the new and revised definitions as requested.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	
Document Name	

Comment

In support of NPCC RSC comments.

Are these comments for the SAR drafting team or the Standards drafting team per the question’s text?

Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries

Request that the SDT post the draft revisions as “red-line to last approved” rather than “to last posted.” This expectation is consistent with posting of other NERC Standards and earlier postings of CIP updates.

Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	
Document Name	

Comment

Cleco supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	
Document Name	

Comment

See MidAmerican Energy Company comments from Darnez Gresham.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Berkshire Hathaway Energy - MidAmerican Energy Co. - 3

Answer	

Document Name

Comment

Planned and Unplanned changes language should be added to the Implementation Plan, similar to the language included in previous CIP implementation plans. *(See Implementation Plan For Version 5 CIP Cyber Security Standards, November 7, 2011; Implementation Plan for Version 5 CIP Cyber Security Standards, October 26, 2012; and Implementation Plan - Project 2014-02 CIP Version 5 Revisions, January 23, 2015.)*

Likes 0

Dislikes 0

Response

Sing Tay - OGE Energy - Oklahoma Gas and Electric Co. - 6, Group Name OKGE

Answer

Document Name

Comment

OKGE supports EEI's comments especially in regards to the proposed new and modified terms that are not being balloted.

Likes 0

Dislikes 0

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer

Document Name 2016-02_Virtualization_Unofficial_Comment_Form_R2_RF_FINAL.docx

Comment

See Question 14 in the attached document

Likes 0

Dislikes 0

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

Gerry Adamski - Cogentrix Energy Power Management, LLC - 5

Answer

Document Name

Comment

We support NPCC TFIST's comments as found below:

Are these comments for the SAR drafting team or the Standards drafting team per the question’s text?

Request clarification on cloud connectivity. The SAR explicitly excludes cloud connectivity. However, entities may use cloud connectivity. Does this divergence create a perverse incentive for entities to move to the cloud so assets/systems in the cloud are out of audit scope? See CIP-007 R2 – does not include patching in the cloud. And requirements that deal with physical boundaries

Request that the SDT post the draft revisions as “red-line to last approved” rather than “to last posted.” This expectation is consistent with posting of other NERC Standards and earlier postings of CIP updates.

Since CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?

Likes 0

Dislikes 0

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller, Group Name MEAG Power

Answer

Document Name

Comment

MEAG Power adopts the Southern Company comments.

Likes 0

Dislikes 0

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer

Document Name

Comment

Because the Technical Rationale documents are being removed from the Standard template, we would suggest that links to these documents be incorporated into each Standard for ease of reference.

Likes 0

Dislikes 0

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer

Document Name

Comment

BC Hydro welcomes the opportunity to comment and expresses gratitude for SDT's efforts to continue to move towards a practical and industry-wide acceptable solution to the technical question of Virtualization faced by the Entities in the NERC CIP domain. BC Hydro looks forward to the enhancements of the identified items in glossary of terms for a better understanding and successful implementation.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE does not agree all proposed changes are specific to virtualization. The revisions to CIP-010 R1.1, for example, are not clear how removing the requirement to maintain baseline documentation is related to permitted virtualization architecture or the security risks associated with virtualization technologies. Texas RE respectfully requests the SDT’s reasoning for how each of the proposed changes address security risks and permitted architecture specific to virtualization.

Likes 0

Dislikes 0

Response

Brian Tooley - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer

Document Name

Comment

SIGE proposes the following for CIP-003 Attachment 1 Section 5, 5.1 and 5.2.

“Controls that maintain the state of the operating system and software such that it is in a known state prior to use;”

In CIP-006, in the Applicable Systems column for Part 1.1, the term “hosting” is used in “SCI without ERC hosting Medium Impact BCS,” but “hosting” has been changed to “supporting” in other places.

Similarly, in CIP-009, in the Applicable Systems column for Parts 2.1 and 2.2, the term “hosting” is used in “SCI hosting Medium Impact BCS at Control Centers or their” but “hosting” has been changed to “supporting” in other places.

Likes 0

Dislikes 0

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name Southwest Power Pool Standards Review Group (SSRG)

Answer

Document Name

Comment

SPP wants to thank the drafting team for their work on these proposed revisions.

Recommend correcting the spelling error in CIP-005 2.6.2 “systerms” should be “systems”.

Recommend spelling the SCI acronym out on page 5 since it is the first use of the term.

Recommend changing reference “1.4” to “1.3” on page 32 under the VSL section.

Recommend researching and adding in the word “Cyber” in all areas that reference “Cyber Security Patch” for document consistency.

Likes 0

Dislikes 0	

Response

Eli Rivera - CenterPoint Energy Houston Electric, LLC - NA - Not Applicable - Texas RE

Answer	
Document Name	

Comment

CEHE proposes the following for CIP-003 Attachment 1 Section 5, 5.1 and 5.2.

“Controls that maintain the state of the operating system and software such that it is in a known state prior to use;”

In CIP-006, in the Applicable Systems column for Part 1.1, the term “hosting” is used in “SCI without ERC hosting Medium Impact BCS,” but “hosting” has been changed to “supporting” in other places.

Similarly, in CIP-009, in the Applicable Systems column for Parts 2.1 and 2.2, the term “hosting” is used in “SCI hosting Medium Impact BCS at Control Centers or their” but “hosting” has been changed to “supporting” in other places.

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	
Document Name	

Comment

We concur with the SDT’s goal of revising the CIP standards to address virtualization, provide more options for Responsible Entities to remain compliant and ensure reliability while utilizing new and different technologies, and be objective-focused. To that end, we applaud the SDT’s continued work and effort on this project.

With that said, after considerable time reviewing the proposed revisions and additions, and much time consulting with and debating peers over the changes, we have arrived at the conclusion that it might be a mistake to attempt virtualization solely through revision of the existing CIP requirements. Currently the revisions are focused on setting the requirements at a level high enough to be technology agnostic, where they can be applied regardless of whether a mixed-trust approach is used. While laudable in theory, the result so far seems to be extensive revisions requiring multiple new definitions, all of which are somewhat confusing in their entirety and potentially difficult to implement properly due to the confusion. Further the extent of the changes presents opportunities for auditors in future to arrive at undesired intepretations. Compounding the issue is that these changes are being made to allow for options which not all Responsible Entities will avail themselves of – and in fact possibly very few will, at least in the near future. Again, we support the SDT’s goal of allowing Responsible Entities more options for maintaining reliability and compliance. But we question how worthwhile it is to enact a raft of changes on existing requirements where only a minority of companies will be seeking to use them.

Accordingly, instead of revising every existing CIP requirement, we believe that a new CIP standard should be enacted, along with any necessary changes to CIP-002 R1 for scope and CIP-005 R1 for ESP, to address virtualization requirements. This can meet all the goals of the SDT while minimizing impact to existing CIP requirements and compliance programs.

We thank the SDT for this opportunity to provide comment and feedback.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	
Document Name	

Comment

We would like to thank the SDT for their hard work on this project and addressing industry comments.

Likes 0	
Dislikes 0	

Response

Susan Sosbe - Wabash Valley Power Association - 1,3

Answer	
Document Name	

Comment

This approach is highly based on a Zero Trust Model. While Zero Trust and it’s assumption of assuming no network edge is an excellent security approach, it is necessary to ensure that a discrete boundary defines the edge of the auditable network. The current definitions significantly blur this border introducing uncertainty into what will be audited under the CIP standards and introduces opportunity for significantly different viewpoints between auditors and entities regarding the boundary of what will be subject to NERC compliance standards. The definitions are also too dependent on interpretation that is not enforceable as the appropriate guidelines are no longer a part of the standard. We do support adopting definitions and standards that support virtualization.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	
Document Name	

Comment

AZPS would like clarification on the PCA Definition regarding the phrase “actively remediated” and what that entails?

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	
Document Name	

Comment

‘Where technically feasible’ -> ‘Per system capability’

MRO Comment: There are instances of ‘per system capability’ replacing ‘where technically feasible’ that could allow for fewer protections for those BCS. The ROP requires that TFEs require “Compensating and mitigating measures” (NERC ROP Appendix 4D). This is no longer required and limits compliance monitoring. (Consider an EACMS or PACS, which do not require logical isolation, not requiring authentication [Part 5.1] or limiting authentication attempts [Part 5.7]. This poses an increased risk.)

Recommendation: Modify the language of the requirements beyond just replacing ‘where technical feasible’ with ‘per system capability’ to better address risk posed by the lack of the required controls.

Likes 0	
Dislikes 0	

Response

Josh Johnson - Lincoln Electric System - 1

Answer	
Document Name	

Comment

Additional minor and conforming recommendations:

CIP-006 Table R2 part 2.2 - Under Applicable Systems, typo, "EERC" meant to be read as ERC.

CIP-006 Table R3 part 3.1 - Under Applicable Systems, consider removing bulleted SCI applicability and include as a single statement at the bottom of the column for consistency.

CIP-007 Table R1 part 1.3 & Table R4 part 4.2 - Under Applicable Systems, the second bullet "External Routable Connectivity" can be changed to ERC for consistency.

CIP-009 Table R2 part 2.1 & 2.2 - Under Applicable Systems, to improve clarity consider removing 'SCI hosting High or Medium Impact BCS at Control Centers or their associated EACMS/PACS' as these would be included in High and Medium impact BCS in an All-In scenario while 'SCI identified independently supporting an Applicable System Above' covers the independently identified scenario.

Likes 0	
Dislikes 0	

Response

Ronald Bender - Nebraska Public Power District - 5

Answer	
Document Name	

Comment

We concur with the SDT’s goal of revising the CIP standards to address virtualization, provide more options for Responsible Entities to remain compliant and ensure reliability while utilizing new and different technologies, and be objective-focused. To that end, we applaud the SDT’s continued work and effort on this project. While there are several negative comments listed above, we also feel that CIP-002, 005, 007, and 010 are also close to an acceptable revised state.

While the proposed revisions are made with the intent of allowing Responsible Entities more options to achieve compliance, the inclusion of multiple new and revised terms and requirement language across all CIP requirements gives the appearance of more complexity and thus more difficulty in achieving compliance. This may (or may not) only be an issue of optics but optics are important. The goal of providing Responsible Entities more options for compliance must not also detract from the goal of ensuring that the requirements are understandable and explainable to a wide audience.

We thank the SDT for this opportunity to provide comment and feedback.

Likes 0	
Dislikes 0	

Response

Clarice Zellmer - WEC Energy Group, Inc. - 5

Answer	
Document Name	

Comment

See MRO-NSRF and EEI Comments

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	
Document Name	

Comment

CIP-005-8 R1.2 – Has been revised to incorporate requirements for "controlled communications" to and from Management Interfaces. Additional clarity should be provided for the "controlled communicaiton" concept, as currently drafted there is an elevated risk of incorrect implementation by entities due to not adequately interpreting the requirement.

CIP-005-8 R2.6.2 - Has been revised to incorporate requirements for "controlled communications" to and from Management Interfaces. Additional clarity should be provided for the "controlled communicaiton" concept, as currently drafted there is an elevated risk of incorrect implementation by entities due to not adequately interpreting the requirement.

CIP-007-7 R4.1 - The SDT may have struck necessary language when “at the BES Cyber System level (per BES Cyber System capability) or a the Cyber Asset level (per Cyber Asset capability) was removed from CIP-007-6.

Likes 1	Associated Electric Cooperative, Inc., 1, Riley Mark
Dislikes 0	

Response

Katie Connor - Duke Energy - 1,3,5,6 - SERC,RF

Answer	
Document Name	

Comment

Duke Energy appreciates the efforts of the SDT to continue to incorporate feedback and drive towards an implementable, sustainable set of requirements and definitions. Duke has proposed a number of definition changes that we believe are foundational to the success of this effort.

Duke Energy is voting negative on the non-binding poll related to the VRFs and VSLs based on the dependency on definitions and other related comments captured in comment submittals for questions 1 – 13.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	

Document Name	
Comment	
Xcel Energy thanks the drafting team for their hard work and dedication to making the utilization of virtualized systems in CIP environments more effective and flexible. We generally support your efforts and believe the team is on the right track.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name CHPD	
Answer	
Document Name	
Comment	
The trend with the CIP standards has been to change from requiring a specific control to address a cyber security objective to requiring the RE to achieve a cyber security objective. For example, in CIP-007-3, the RE was required to implement antivirus on in-scope CAs to mitigate the threat of malicious software. CIP-007-5 changed this to require the RE to deploy methods to deter, detect or prevent malicious code. This gave the RE the ability to choose the best control for the actual objective (malicious code protection) as opposed to requiring the entity to implement specific control (antivirus) that may not be suitable in all cases. The same can be said for the proposed revisions to ESPs, rather than requiring the specific control of firewalls to act as EAPs for an ESP, the SDT is revising the requirement to grant the RE the ability to select the control best suited to their environment to achieve the cyber security objective (logical isolation). The SDT should use the same objectives based approach with side-channel threats and create requirements that require the RE to design and implement controls that mitigate the threat of side-channel attacks, rather than force entities to implement the specific control of CPU/memory isolation, which is certainly one option, but not the only one. Other controls that would be effective is network isolation of the SCI and its VCAs, whitelisting, or more organizational control to prevent information disclosure (such as randomizing data in memory). Additionally, the CIP standards already address several of the most important controls to prevent side-channel attacks, namely, regular security patching, ports and services hardening, and restricting user access based on need.	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
Reclamation appreciates the SDT's efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the SDT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	
Document Name	Dominion Enegy additional Virtualization comments.docx
Comment	
Please see the attached file with graphics.	
Likes 0	
Dislikes 0	
Response	

Comments Submitted by Lakeland Electric (JEA was originally expected to submit these comments)

1. Are the two options for identification of SCI within CIP-002 clear and is it understood that when SCI is included in the CIP Systems that it is treated like the CIP System, it is a part of for CIP Requirement Applicability?

☒ Yes
☐ No

Comments: **look at applicability

2. The Applicable Systems column may include “SCI identified independently…” Is this clear or is additional clarification (such as “SCI identified as supporting, but not part of…”) needed?

☐ Yes
☒ No

Comments: Need to combine and include both (because ‘independently’ is listed throughout standards and needs to be defined). Example: “SCI identified IDENPENDENTLY as supporting, but not part of….”

3. The SDT modified the ERC definition to reference “outside the asset containing”. This is to allow scoping based on connectivity of the logging systems as required by CIP-007 Requirement R4 as well as the scoping of requirement parts in CIP-004 and CIP-006 based on risk. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: This definition of ERC (by including the new definition of CIP System) extends ERC requiremetns to EACMs and PACs and transient cyber assets. Should be limited to environments that control and monitor BES.

4. The SDT proposes that the modified ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: As the proposed change extends ESP application to CIP Systems (which include EACMs and PACs and transient cyber assets). This application of ESP must be limited to assets impacting BES Control and Monitoring Operations.

5. The SDT modified the IRA definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: IRA definition is applied to CIP Systems which requires application of IIRA to TCA, EACMS, and PACS

6. The SDT modified the Management Interface definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: Is Management interface the Virtual Management Consoles or ILO.

7. As discussed in the CIP Definitions and Exemptions Technical Rationale (TR), the SDT believes that the use of configurations or policy in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments:

8. The SDT added new and revised several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: Deviates from industry standard terms such as used in NIST.

9. The SDT revised CIP-002 based on industry comments. Do you agree with the proposed changes to the CIP-002 Reliability Standard? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: No value addition to current CIP process and adds confusion to CIP asset identification process. If the intent is just clarify VCA, then adding the definition should be more than sufficient.

10. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: No value addition to current CIP process and adds confusion to CIP asset identification process. If the intent is just clarify VCA, then adding the definition should be more than sufficient.

11. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP-007 requirements and improve to risk based compliance.

12. The SDT revised CIP-010 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP-010 requirements and improve to risk based compliance.

13. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 (conforming changes) based on industry comments. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP requirements and improve to risk based compliance.

14. Please provide any additional comments for the SAR drafting team to consider, if desired.

Objective of this SAR was to improve CIP standards to allow use of new technologies such as Cloud where appropriate and improve CIP compliance. Unfortunately, this standard stifles any innovation and forces the industry to use obselence.

- SDT classifies all CIP standards as same risk, which defeats the objective of creating a risk based compliance program.
- Adds a level of complexity and a lack of clarity that would make implementation difficult and result in increased violations without an increase in security.
- Move away from risk-based standards by not segregating assets (such as EACMS, PACS, and TCA) in definitions such as those for CIP System and ERC.
- Do not accomplish the goal and deviate from the original purpose of the SAR: to eliminate the language inherent in V5 that has made it difficult to go virtual. In fact, they may limit or handicap an entity’s ability to go virtual.
- This standard does not add any value to CIP standards as all what is being accomplished by these changes can easily be accomplished by current standards. If the intent is to clarify the application of Virtual systems, then SDT or ERO should release an application white paper.

Comments Submitted by Orlando Utilities Commission (JEA was originally expected to submit these comments)

1. Are the two options for identification of SCI within CIP-002 clear and is it understood that when SCI is included in the CIP Systems that it is treated like the CIP System, it is a part of for CIP Requirement Applicability?

☒ Yes
☐ No

Comments: **look at applicability

2. The Applicable Systems column may include “SCI identified independently…” Is this clear or is additional clarification (such as “SCI identified as supporting, but not part of…”) needed?

☐ Yes
☒ No

Comments: Need to combine and include both (because ‘independently’ is listed throughout standards and needs to be defined). Example: “SCI identified IDENPENDENTLY as supporting, but not part of….”

3. The SDT modified the ERC definition to reference “outside the asset containing”. This is to allow scoping based on connectivity of the logging systems as required by CIP-007 Requirement R4 as well as the scoping of requirement parts in CIP-004 and CIP-006 based on risk. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: This definition of ERC (by including the new definition of CIP System) extends ERC requiremetns to EACMs and PACs and transient cyber assets. Should be limited to environments that control and monitor BES.

4. The SDT proposes that the modified ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: As the proposed change extends ESP application to CIP Systems (which include EACMs and PACs and transient cyber assets). This application of ESP must be limited to assets impacting BES Control and Monitoring Operations.

5. The SDT modified the IRA definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: IRA definition is applied to CIP Systems which requires application of IIRA to TCA, EACMS, and PACS

6. The SDT modified the Management Interface definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: Is Management interface the Virtual Management Consoles or ILO.

7. As discussed in the CIP Definitions and Exemptions Technical Rationale (TR), the SDT believes that the use of configurations or policy in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments:

8. The SDT added new and revised several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: Deviates from industry standard terms such as used in NIST.

9. The SDT revised CIP-002 based on industry comments. Do you agree with the proposed changes to the CIP-002 Reliability Standard? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: No value addition to current CIP process and adds confusion to CIP asset identification process. If the intent is just clarify VCA, then adding the definition should be more than sufficient.

10. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: No value addition to current CIP process and adds confusion to CIP asset identification process. If the intent is just clarify VCA, then adding the definition should be more than sufficient.

11. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP-007 requirements and improve to risk based compliance.

12. The SDT revised CIP-010 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP-010 requirements and improve to risk based compliance.

13. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 (conforming changes) based on industry comments. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

☐ Yes
☒ No

Comments: How does it improve current CIP requirements and improve to risk based compliance.

14. Please provide any additional comments for the SAR drafting team to consider, if desired.

Objective of this SAR was to improve CIP standards to allow use of new technologies such as Cloud where appropriate and improve CIP compliance. Unfortunately, this standard stifles any innovation and forces the industry to use obselence.

- SDT classifies all CIP standards as same risk, which defeats the objective of creating a risk based compliance program.
- Adds a level of complexity and a lack of clarity that would make implementation difficult and result in increased violations without an increase in security.
- Move away from risk-based standards by not segregating assets (such as EACMS, PACS, and TCA) in definitions such as those for CIP System and ERC.
- Do not accomplish the goal and deviate from the original purpose of the SAR: to eliminate the language inherent in V5 that has made it difficult to go virtual. In fact, they may limit or handicap an entity's ability to go virtual.
- This standard does not add any value to CIP standards as all what is being accomplished by these changes can easily be accomplished by current standards. If the intent is to clarify the application of Virtual systems, then SDT or ERO should release an application white paper.

Overall Comments:

The June 2021 redlines are an improvement over the previous version; however, the modifications:

- Add a level of complexity and a lack of clarity that would make implementation difficult and result in increased violations without an increase in security.
- Move away from risk-based standards by not segregating assets (such as EACMS, PACS, and TCA) in definitions such as those for CIP System and ERC.
- Do not accomplish the goal and deviate from the original purpose of the SAR: to eliminate the language inherent in V5 that has made it difficult to go virtual. In fact, they may limit or handicap an entity's ability to go virtual.
- This standard does not add any value to CIP standards as all what is being accomplished by these changes can easily be accomplished by current standards. If the intent is to clarify the application of Virtual systems, then SDT or ERO should release an application white paper.

- Definitions
- **CIP System** - this extends the definition to include EACMS, PACS, and TCA. When applied in standards or other definitions, it expands the scope significantly. Systems such as SIEM and PACS are supposed to control and Monitor an enterprise and separate instances limit the ability of security operations to respond to active incidents. Applying CIP System definitions will expand scope to environments where impact will limit security and will be detrimental.
- We recommend this definition be removed and appropriate devices groups such as EACMs, PACS be directly used in order to avoid any confusion.
- **ERC** – by including "ability to connect to a CIP System," in the definition of ERC, this extends ERC requirement to EACMS, PACS, and TCA. Should be limited to environments that control and monitor BES as was the scope of the SAR. Also, the statement "outside the asset containing the CIP system" may need clarity – where does this draw the line? **ESP** – as proposed, it appears this may extend the definition of ESP to CIP Systems (including EACMS, PACS, and TCA), but application of ESP must be limited to assets impacting BES control & monitoring operations. EACM, PACS and TCA should not be required to maintain an ESP as they are support assets and exists in homogeneous corporate environment. This change assumes the same risks for all assets/environments and fails to deliver a Risk based application.
- **Intermediate Systems** – should not be on the same network for which it restricts the access or any of the devices it protects. This definition is understood.
- **IRA** – Does this now apply to all within ESP and IRA applies to any of the CIP Systems? Why does the last bullet so specific and not make reference to "asset point?" Overall, definition is understood, but complicated.
- **Management Interface** – we need more clarity, for example does this include ILO as management interface? Is it a vector or device (ESXI console)?

  - **TCA** – this definition/inclusion of the virtual environment is confusing. If the TCA is on the same network, then it will bea PCA or if separate then it will have to use a jump host. How will this apply to Entity's virtual workstations? Would we have to prove the virtual system has ESP and ERC compliance? Need clarity.

- CIP-002
  - It is clear that we are given two options: (1) SCI included in CIP Systems and treated as the[MDD-DCC1] CIP System; and (2) SCI identified independently; just to be clear, based on "each asset", are we also able to do a hybrid model in which some SCI is include and some SCI is identified as independent? It appears to be the case.
  - New standard allows for either zero trust method (protect close to asset) or former edge-based method (ESP and firewalls); however if we want to continue with the edge-based method, we don't want to high water mark everything
    - i.e. Does this mean the corporate host may become SCI for CIP?
    - That CIP System is really giving us a problem in terms of ERC
  - We have concern that corporate host may become SCI; Will the SIEM systems (EACM) not allowed to share Processor and Memeory, that would require them to maintain separate SCI and hence critical requirements such as SIEM can never be migrated to Cloud instance and can never take advantage of any new technology. Furthermore, such a standard assumes that Risks for the EACM and BES assets is exactly the same, and fails to deliver a Risk based application which was the FERC manadate. SDT can specify the security requirements for Shared SCI in a manner that addresses the risk and hence allowing Entities to benefits from transitioning to more advanced technology for EACMs and Data storage, which will significantly improve security.

- CIP-005
  - Allows us to keep firewall or take protection closer to the asset
  - Part 1.2 – only applies to firewall because "identified independently"
  - Part 1.4 – addresses ability to have a "super ESP" between 2 control centers and protect communication between the two
  - Part 2 – ok with requirement; but is there any other way for vendors to access that doesn't involve intermediate host?

- CIP-007
  - Part 1.1 – if this requires EACMS connect to TCA, we may have a problem – includes EACMS, PACS, & PCA except we've high water marked our PACS as high
    - What is meant by "or services if unable to determine ports" – is this for dynamic port ranges or for cloud services to randomly change ports?
  - Part 1.2 – "non-programmable communications components inside PSP & ES," what is this? Is this encouraging USB port locks?
  - Part 1.4 – If you choose independent SCI, can't run ES Cyber systems along with non-CIP
    - NOTE: JEA does not agree the requirements are risk-based.; should be differentiated because this limits our availability to use virtual technology
    - How can we verify that memory is not shared?

- CIP-010
  - Need to review

- CIP-011
  - Ok for the most part

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Response to Comments

Project 2016-02 Modifications to CIP Standards
Draft 2 Posting ending September 1, 2021

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Jordan Mallory (404-446-2589).

Background Information

Project 2016-02 (1) addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and (2) considers the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for Standard Drafting Team Consideration (V5TAG Transfer Document).

The V5TAG, which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP Version 5 standards and to support industry's implementation activities. During the V5TAG's activities, it identified certain issues with the CIP Reliability Standards that would be better addressed by a standard drafting team (SDT) for the CIP Reliability Standards. The V5TAG developed the CIP Version 5 Transition Advisory Group Issues for Consideration document to formally recommend that the SDT address these issues and consider modifications to the standard language during the standards development process. Among other issues, the V5TAG stated "The CIP Version 5 standards comments.

There were 93 sets of responses, including comments from approximately 218 different people from approximately 137 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Question 1.

Are the two options for identification of SCI within CIP-002 clear and is it understood that when SCI is included in the CIP Systems that it is treated like the CIP System, it is a part of for CIP Requirement Applicability?

Q1 Comment Themes

- **The options are mostly clear and acceptable with the exception of the phrase "independent SCI supporting"**
- **The term 'SCI' is still unclear and ambiguous**
- **Does not agree that the two options for identification of SCI are clear. The distinction between SCI included in a BES Cyber System (BCS) and SCI operating independently adds an unnecessary level of complexity to the standards**

SDT Response: Thank you for your comments. The SDT agrees with this theme that much more clarity around SCI is needed and has taken a different and simplified approach for the next draft. The two options remain for entities to either:

1) dedicate a virtualized infrastructure to hosting Virtual Cyber Assets (VCA) of the same CIP impact rating or 'associated with' the same impact rating (i.e., "all-in") or,
2) share the virtualized infrastructure hosting Virtual Cyber Assets (VCA) of different CIP impact ratings or non-CIP impact rated (previously known as "SCI Identified independently").

The terminology of this latter case ("identified independently") will no longer be used. In order to simplify these options, the term SCI will be redefined to ONLY refer to the second option.

For the "all-in" scenario, the virtualized infrastructure hardware components are now simply Cyber Assets that are a part of the systems they are hosting, such as BCAs in a BCS, or as Cyber Assets in an virtual EACMS, PACS, or PCA. In this scenario, every VCA hosted on the Cyber Assets, and the Cyber Assets themselves, are of the same impact rating. *There is no SCI in this option*. The SDT believes this is the way most entities with existing virtual systems have identified and categorized their virtual infrastructures to date and this will allow that to remain unchanged.

The SDT in response to this comment theme has modified the SCI definition so that it ONLY applies to the second scenario, where the "S" in "SCI" means the underlying hardware *is shared among VCAs of differing impact levels* (i.e., 'mixed mode'). This simplification allows for distinct scoping of new additional requirements for the proper isolation required as well as restricting access to the management plane where the isolation is configured.

To recap:

- If the entity implements BCS and any associated EACMS or PACS or PCAs as VCAs on an underlying hardware infrastructure, and all is treated as or 'associated with' the same (highest) impact rating, this is "all-in" and the underlying hardware is identified as Cyber Assets that may also be BCAs in a BCS or part of the EACMS or PACS they host. There is no SCI in this scenario. No CIP-002 recategorization is required.
- If the entity hosts VCAs of varying impact levels and wishes to use the security controls to keep each impact level environment isolated from each other, then the underlying hardware is identified as SCI and additional requirements for such isolation are required for this environment.

Question 2.

The Applicable Systems column may include “SCI identified independently…” Is this clear or is additional clarification (such as “SCI identified as supporting, but not part of…”) needed?

SDT Response:

Thank you for your comments. Most entities answered this question, which is closely related to Q1 with shared themes from Q1. Please see Q1 responses for the SDT response to those themes.

Question 3.

The SDT modified the ERC definition to reference “outside the asset containing”. This is to allow scoping based on connectivity of the logging systems as required by CIP-007 Requirement R4 as well as the scoping of requirement parts in CIP-004 and CIP-006 based on risk. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Q3 Comment Theme:

- **Use of "asset" for scoping is unclear**

SDT Response: Thank you for your comments. The SDT agrees with comments that the “asset containing” is not defined precisely enough for use in this foundational scoping term of ERC. While the intent of ERC is to restrict the scope of certain requirements for assets/sites that do not have the requisite type of communications, this has traditionally been accomplished by using the ESP as the demarcation point of ERC, not the “asset containing”. The SDT will return ERC to being ESP-based. In addition, the ERC definition essentially mirrors the currently approved definition with one change of replacing concepts of “inside or outside” an ESP to “through its ESP” to better position it for Zero Trust architectures that are not strictly network perimeter based.

Q3 Comment Theme:

- **Expands the existing definition by changing from “BES Cyber System” to “CIP System” and by changing from “to access” to “to communicate”.**

SDT Response: Thank you for your comments. The SDT agrees and has reinstated the BES Cyber System as the subject of ERC definition and reverted to the currently approved “access” language. The ERC definition now essentially mirrors the currently approved definition with one change of replacing the concepts of “inside or outside” an ESP to “through its ESP” to better position it for Zero Trust architectures that are not strictly network perimeter based.

Question 4.

The SDT proposes that the modified ESP definition can be used for both traditional firewall based networks, as well as future networks such as zero trust. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Q4 Comment Theme:

- **EACMS appears to be required**

SDT Response: Thank you for your comments. The SDT agrees with the commentors. The “enforced by an EACMS” phrase, while meant to help define the extent of the ESP especially in Zero Trust architectures, did require an EACMS in order for an ESP to exist. As commenters rightly pointed out, this negated being able to define ESPs for isolated networks. The SDT addressed this concern by reinstating the current ESP definition and added a second component , "; or a logical boundary defined by one or more EAPs" to address zero trust.

Q4 Comment Theme:

- **ESP does not include routable scoping**

SDT Response: Thank you for your comments. The SDT agrees and worked routable protocol scoping back into the definition.

Q4 Comment Theme:

- **PCA may be redundant in ESP definition**
- **ESP no longer includes boundary**

SDT Response:Thank you for your comments. The SDT agrees with the various comments in this theme, which revolved around being able to define an ESP around isolated networks that do not have ERC but still need an ESP for defining PCAs, knowing the extent of TCA connections, etc. While the SDT's draft 2 proposed definition was more objective in order to incorporate rather different security models (traditional 'castle/moat' perimeter vs. Zero Trust), the SDT agrees the definition needs more specificity in order to not lose its other boundary-like functions that it fulfills even in isolated networks that do not have external connectivity. The SDT also agrees that the PCA definition adequately defines those Cyber Assets, therefore the ESP definition doesn't need to specifiy it includes or groups PCAs.

Q4 Comment Theme:

- **The word "policy" is not well understood**

SDT Response: Thank you for your comments. The SDT agrees that 'policy' needs more context in order to be well understood whether it is a business or administrative policy document or a technical configuration of a firewall policy. The SDT addressed these comments by removing the term 'policy' where it was intended to reflect technical controls, (e.g. software designed networks, instruction detection policies, or firewall rules/policies, etc.) and replaced it with 'configuration or settings'.

Q4 Comment Theme:

- **The use of 'CIP Systems' in the definition is too broad**

SDT Response: Thank you for your comments. The SDT agrees as all types of 'CIP Systems' are not required to be within an ESP. While not a requirement in CIP-005, it is an implication of the definition. The SDT eliminated this new definition and its reference from the ESP definition.

Question 5.

The SDT modified the IRA definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Q5 Comment Theme:

- **The protocol conversion bullet could expand scope beyond the intent (Control Center operator to field device as IRA). The second bullet point is unclear and ambiguous.**

SDT Response: Thank you for your comments. The SDT asserts that the 2nd bullet was correct but agrees it was complex and has made modifications to simplify it. The intent is to cover the situation where an interactive user is using a routable protocol (i.e., an IP address) and is able to access a BES Cyber System and operate or configure it, often called terms such as "engineering access", even if the BES Cyber System itself uses only non-routable communications, such as a serial cable to a console port. In this case, the CIP-005 R2 controls should apply to the routable portion of the communications, and this bullet in the IRA definition is designed to capture that scenario, but with simplified language in our next draft.

Q5 Comment Theme:

- **"real-time" needs deletion/clarification/capitalization.**

SDT Response:

Thank you for your comments. The SDT agrees. The intent was to further define that 'interactive' access was in 'real-time', not access a user has programmed for a future time such as a scheduled batch job that runs when the user is no longer logged in. While this is a risk, its is not the subject of CIP-005 R2's security controls, which are designed for a real-time, interactive user. Batch jobs can't execute through a "pane of glass" interface of a typical Intermediate System, or enter a user's current code from a physical token, or receive a text with a one-time-password from the user's phone. Therefore, IRA is not all-inclusive but is designed around this high risk area of interactive, 'real-time' interaction with a BES Cyber System and isolating the remote user's machine (through an Intermediate System), strongly authenticating the user (through multi-factor authentication), and protecting the session's traffic over less trusted networks (encryption from the Intermediate System to the client). However, as commenters pointed out, the term 'real-time' was confusing or unnecessary, so the SDT deleted it from the definition.

Q5 Comment Theme:

- **Add "IRA does not include system-to-system process communications" back to the definition.**

SDT Response: Thank you for your comments. The SDT believes this comment was made related to the above comment concerning the term 'real-time' in the definition. There was a sense of if the term 'real-time' stayed in, this phrase needed to be added back to state 'real-time' communications did not include system-to-system communications (e.g., a system polling an RTU). The SDT removed the term 'real-time' to respond to these comments and asserts that the first phrases of the definition precludes system-to-system communications without an explicit negative phrase in the definition.

Question 6.

The SDT modified the Management Interface definition based on industry comments. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Q6 Comment Theme:

- **The second bullet concerning "lights out" needs clarification/is unclear/is vendor specific.**

SDT Response: Thank you for your comments. The SDT does not assert that "lights out management" is a vendor-specific term, but due to the number of comments the SDT changed this second bullet back to the language that had been proposed in the SDT's draft 1 definition of 'Management Module' as suggested by many in the comments.

Q6 Comment Theme:

- **Ambiguity about the intent of the 'user interface, logical interface, or dedicated physical port**

SDT Response: Thank you for your comments. The SDT agrees and replaced this phrasing with "An administrative interface on a Shared Cyber Infrastructure or Electronic Access Control or Monitoring System that…" which is clearer as to the intent of a Management Interface rather than a description of the several forms it may take.

Question 7.

As discussed in the CIP Definitions and Exemptions Technical Rationale (TR), the SDT believes that the use of configurations or policy in the modified ESP definition can reduce the burden of documenting ESPs in a zero trust environment. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Q7 Comment Theme:

- **Agreement/Disagreement with reduced documentation burden**

SDT Response: Thank you for your comments. Most of the comment themes for Q7 were either agreement or disagreement with the reduction in documentation burden based on the overall ESP themes reported in Q4. See Q4 responses to those specific themes. The SDT would like to take this opportunity to clarify the question and its position, which is in agreement with many points commenters made.

The goal of CIP-005 R1 has, from the beginning of CIP-005, been to establish a "policy or configuration" of who/what can communicate with a BCS or its associated PCA's inside a protected network (ESP) and ensure that each element of that policy/configuration allowing communication is necessary; that it implements the security principle of least privilege. This is accomplished in today's more prescriptive perimeter-based architecture by having a documented list of ESPs, which leads to a documented list of EAPs, which then leads to documentation of the policy/configuration within each EAP which is the basis for determining whether the ESP is compliant with the intent of the requirement. So today, ESPs and EAPs are mechanisms for getting to the actual policy/configuration of what is allowed to communicate across the boundary. That intent does not change; the SDT's approach states the eventual policy/configuration as the direct object of the requirement rather than indirectly through documented lists of ESPs and EAPs.

However, the SDT is attempting to change the standards so that other models such as Zero Trust (ZT) are not prohibited or discouraged by overly prescriptive language. As several commenters pointed out, in ZT the number of ESP/EAPs will increase as ESPs "shrink" from protecting a network segment down to protecting a single resource or service, so in that sense going directly to the policy/configuration reduces the burden of the intermediate step of documenting ESPs as the number of those may increase exponentially in full ZT implementations. As other commenters pointed out, ZT with its more granular access control will potentially greatly increase the number of policy/configuration statements of "what can talk to what", so it does not reduce documentation in that regard. The SDT agrees.

Question 8.

The SDT added new and revised several defined terms to incorporate virtualization and future technologies within the CIP Standards. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

NOTE: Many comments for Q8 referred back to issues with the specific questions on specific definitions in Q1-6. Please see responses to those issues in the appropriate question above.

Q8 Comment Theme:

- **Intermediate System: The statement "The Intermediate System must not be located inside the Electronic Security Perimeter" should be retained**

SDT Response: Thank you for your comments. The SDT disagrees and asserts that the "where" of the Intermediate System is a requirement that is embedded within the current definition. If an entity places the Intermediate System inside an ESP such that "public" encrypted traffic is allowed in from yet-to-be authenticated users, that should be a violation of a requirement, not simply not meeting a definition. The SDT removed this phrase from the definition and authored a requirement in CIP-005 R2.6 to address this situation.

Q8 Comment Theme:

- **CIP Systems: Remove "TCA" from "CIP Systems". TCAs are included in the CIP System definition. However, CIP System is used in the definition of ESP.**

SDT Response: Thank you for your comments. The SDT, in response to comments, removed the nested use of "CIP Systems" in other definitions. Upon further analysis, it was then only used in a non-essential clarification in CIP-010 R1.2 that has been removed. The SDT has deleted the proposed term "CIP Systems".

Q8 Comment Theme:

- **Cyber System: Revert back to Cyber Assets or go with generic "cyber system" term, leaving it undefined**
- **Cyber Asset: Consider not excluding SCI, keeping the original**

SDT Response: Thank you for your comments. After mindful consideration of comments, the SDT disagrees that Cyber Asset is now one form an object, with applicable CIP requirements, can take; an inclusive hardware-based electronic device with all the software and data in the device. Virtualization fundamentally breaks the 1:1 tie between hardware resources and the varied and dynamic VCA that may happen to execute on it (be "in the device"). The SDT intent is that the objects of CIP requirements can now take one of three forms: Cyber Assets, Virtual Cyber Assets, or SCI. This term ("Cyber System") was created as an attempt to reduce admistrative burden on Registered Entities by establishing this as shorthand for those three forms so all three do not have to be repeated to update every occurrence of 'Cyber Asset' within all CIP documentation. In addition, in Draft 1, the SDT attempted using the generic words ‘cyber system’ as an undefined term in the exemptions and stakeholder comments were numerous that this term must be a defined glossary term.

The SDT analyzed the comments regarding removal of the exclusion for SCI from the Cyber Asset definition, and after consideration has chosen to retain this exclusion in the Cyber Asset definition for sound cause. If the underlying hardware resource pool of SCI is a “Cyber Asset” then that definition consumes ALL software (VCA) on the SCI. The all-inclusive nature of the Cyber Asset definition is a core issue with SCI scenarios, and the exclusion is necessary to prevent this condition.

Q8 Comment Theme:

- **Protected Cyber Asset (PCA): Additional clarifications on the qualifier of “excluding Virtual Cyber Assets that are being actively remediated prior to introduction to the ESP.”**

SDT Response: Thank you for your comments. The SDT’s intent is this is part of a set of changes to ensure the CIP requirements and definitions do not prohibit or discourage automated means of vulnerability assessment and remediation in virtualized environments (a.k.a “Remediation VLANs”). In these instances, a VCA already resides “in a production environment” but whenever it is instantiated, it is placed on an isolated network where it is assessed against the security policy and remediated as needed to meet the expected security hygiene level before being placed on a production network, all in an automated fashion. However, although during this assessment/remediation process it is isolated from a network perspective, it may for a very brief period of time meet the 2nd part of the proposed PCA definition in that it may be executing on the same hypervisor as a BCS. The SDT asserts that since it is isolated from a network perspective while it is being remediated in an automated fashion, it should not require separate and distinct hypervisor infrastructure for this brief period of time. This is the reason for this exclusionary qualifier in the PCA definition.

Q8 Comment Theme:

- **Overall: Some definitions include requirements on CPU and memory (isolation/shared) and are not future proof**

SDT Response: Thank you for your comments. The SDT intent in these definitions and related requirements is to mitigate the risk unique to virtualization of hardware based ‘side channel’ attacks from other VCAs executing on the same hardware (CPU/Memory). Attacks such as Rowhammer where one process can potentially change code or data in physically adjacent memory belonging to another process, or Spectre/Meltdown where a hardware CPU vulnerability could allow access to other processes are the risk, as a couple examples. The SDT has considered higher level objective language such as “mitigate the risks of side-channel attacks” as suggested by other commenters but finds that to be overly broad. This sharing of physical CPU and memory is a virtualization specific risk that is being mitigated and is specific enough that entities can show affinity rule configurations as evidence of compliance when hosted on SCI. Using such terms may not be ultimately future-proof, but the SDT is having to balance the security objectives with enough specificity that entities know how to comply and how to provide evidence of compliance.

Q8 Comment Theme:

- **PCA: The CPU/memory affinity requirements are problematic in that it essentially places a requirement inside a definition. The implicit requirement is that a BES Cyber Asset cannot share CPU/memory with a non-BCS of the same impact rating or a Protected Cyber Asset.**

SDT Response: Thank you for your comments. After mindful consideration of comments, the SDT disagrees that this is a requirement within a definition. The SDT intent is for it to be each entity's choice whether to 1) employ affinity rules or, 2) separate VCA's of differing impact levels onto separate hypervisors. However, should an entity choose to not employ methods to keep VCAs of different impact levels from executing on the same CPU/memory subjecting those VCAs to hardware-based side-channel attacks, then those VCAs that are not BCAs are properly defined as an associated PCA; creating the need for this language within the PCA definition. If the entity chooses to employ methods to separate VCAs onto different hypervisors or server blades so they do not execute on the same CPU/memory simultaneously, then the risk is mitigated and they no longer meet the definition of a PCA from that perspective. There is no requirement to employ such methods, just the consequence of becoming a PCA if the entity chooses not to.

Q8 Comment Theme:

- **Overall: Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation**

SDT Response: Thank you for your comments. The SDT suggests that posting definitions alone would not give stakeholders the necessary context of how a definition is used within the standards and would hamper stakeholder acceptance. The SDT asserts that posting these together with the applicable Standard changes is a necessary part for gaining stakeholder acceptance, especially for the very context-sensitive technical terms in CIP, is dependent upon having the context of its use within requirements.

Question 9.

The SDT revised CIP-002 based on industry comments. Do you agree with the proposed changes to the CIP-002 Reliability Standard? If not, please provide the basis for your disagreement and an alternate proposal.

NOTE: Several commenters reported they cannot support CIP-002 changes due to concerns with the definition of SCI expressed in Q1. Please see responses to Q1 above.

Q9 Comment Theme:

- **CIP-002 R1 requirements should be restored and all other SCI language in CIP-002 Attachment 1 should be removed**

SDT Response: Thank you for your comments. After the latested modification of the SCI definition (See Q1 above), the SDT agrees and has reverted the CIP-002 requirements to currently approved language. As our scope was virtualization, we only covered the identification of SCI. However, the identification of "all other" types of Cyber Systems other than the BES Cyber Systems (EACMS, PACS, PCAs, SCI, etc.) is a larger issue that should be considered holistically.

Q9 Comment Theme:

- **Concern that in the Exemptions both data communication links and communication networks should be exempt as in currently approved language.**

SDT Response: Thank you for your comments. The SDT's intent was that shortening to the phrase "communication links" included both, but in response to comments the SDT has reincorporating the full language back into the exemptions.

Q9 Comment Theme:

- **Request clarification of capitalization of "High Impact," "Medium Impact" and "Low Impact."**

SDT Response:

Thank you for your comments. The SDT agrees and the capitalization of these terms was reviewed and corrected.

Question 10.

The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

NOTE: Many comment themes in CIP-005 are based on issues with individual definitions (ESP, EAP, IRA, SCI, etc.). For responses to those themes, please see the appropriate question above.

Q10 Comment Theme:

- **Request clarification between Part 1.2 and Part 1.3. Part 1.2 reads "Permit only needed and controlled communications to and from Management Interfaces, and deny all other communications" which seems to include Part 1.3 which reads "Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability."**
- **In addition electronic access controls should be in-place on the Management Interface to only allow the appropriate administrators access to it. The prescriptive and broad ban of traffic from the data plane seems excessive. The separation occurs in cloud-based hosting because the hosting service is the administrator and the tenant is not. For on-premise that is not the case and the administrator and tenant are the same entity.**

SDT Response:

Thank you for your comments. The SDT asserts that having the VCAs, on SCI, not have access to the management plane is a best practice, but agrees with the issues brought up by the commenters. Since a person using IRA to a Management Interface will have the controls of CIP-005 R2 applied, and the overarching R1.2 (now 1.3 due to the reinstatement of 1.1 and the renumbering) permits only needed communications to and from the Management Interfaces with justification, the SDT agrees, and deleted the Draft 2 Part 1.3 language.

Q10 Comment Theme:

- **The host-based firewall exclusion in R1 is not appropriate for objective-based model/needs clarification/may be needed for Zero Trust implementation/should be in Implementation Guidance.**

SDT Response: Thank you for your comments. The SDT agrees. The intent of the exclusion was to avoid the scenario of a BCS being plugged into the Internet with only the internal OS firewall turned on. A compromise of the host through any OS vulnerability was then also a compromise of the firewall itself. It met the higher level objective, but with an insufficient separation of the security control from the object protected. The SDT has deleted the exclusion language and reinstated R1.1 in order to address the issue.

Q10 Comment Theme:

- **Requirement 1.1 includes a new insertion "between intelligent electronic devices", what is an intelligent electronic device?**

SDT Response:

Thank you for your comments. The SDT's intent was to bring forward the exclusion from the low impact scenario where ESPs and firewalls are excluded in very time sensitive applications such as relays communicating with each other for asset protection functions. The term "intelligent electronic devices" is a term of art, but remains undefined and the SDT agrees is an overly generic term. The SDT is proposing to use the NERC Glossary defined term of "Protection System" in its place, and moved the exclusion to Part 1.2 after the reinstatment of Part 1.1.

Q10 Comment Theme:

- **Hall of mirrors is created in R2.1 where an Intermediate System is needed for an Intermediate System**

SDT Response:

Thank you for your comments. The SDT agrees. This was a document error that was only in the clean but not the redline versions of the standard. This has been corrected.

Q10 Comment Theme:

- **R1.6 on detecting malicious communications needs consideration of the "where" in light of Zero Trust and changes to the ESP.**

SDT Response:

Thank you for your comments. The SDT has changed the requirement in response so that it refers to the communications that are entering or leaving an ESP and changed the Applicable Systems column to describe which ESPs – it applies to high impact BCS and medium impact BCS at Control Centers. This should make the requirement focus on specifically what communications need to be detected, but avoids implication of where the technology must reside to do so.

Question 11.

The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

Q11 Comment Theme:

- **Requirement 1.2 need clarification on what "non-programmable communications components located inside both a PSP and ESP" includes.**

SDT Response: Thank you for your comments. The SDT asserts that this is a redline error and is from currently approved CIP-007-6 and is not a change made by this SDT. We apologize that it showed as a change in the redline. It covers, for example, "non-programmable" communication components such as a unmanaged network switch that may not meet the definition of "Cyber Asset" but are still the object of this existing requirement.

Q11 Comment Theme:

- **Request clarification on CIP-007 Part 1.1. Why is this Requirement so technology specific? We refer to "Internet Protocol ports" instead of "ports." There is inconsistency between CIP-007 Parts 1.1 and 1.2 where 1.1 uses "Internet Protocol ports" while 1.2 uses "physical input/output ports" and "network connectivity." We expected consistency.**
- **Under Internet Protocol (IP), the transport layers (e.g. TCP, UDP) create and maintain the ports for the underlying services.**

SDT Response: Thank you for your comments. The SDT agrees that logical ports are at the TCP/UDP level and not IP (per RFC 791). Based on the feedback, the SDT has taken a simplified approach to this requirement by stating it as a clearer objective of system hardening – disable or prevent unneeded routable protocol network accessibility on each Applicable System. This intent is that in the virtualization underlay, the hardware resource pools being managed by hypervisors communicating with each other, the entity can manage unneeded network accessibility by disabling underlay services that are not needed. This also allows entities to achieve the objective at either a port or service level; some unneeded accessibility may be disabled/prevented at a TCP/UDP port level, others by disabling a service in the OS. The objective is to reduce the network attack surface of the Applicable System and no longer prescribes that this be accomplished at either a port or a service level.

The intent of the different 1.1 and 1.2 requirement parts remains in that 1.1 is concerned with operating system (OS) level ports and services, while 1.2 is concerned with physical hardware ports, for example, RJ45 ethernet, USB ports, and DB9 serial ports.

Q11 Comment Theme:

- **Requirement 1.3 is greatly limiting. One objective of virtualization is to optimize the usage of computer resources (CPU, memory, etc.) and this limits the possible gain of using virtualization.**

SDT Response:

Thank you for your comments. The SDT is allowing entity choice on the treatment of computer resources by either considering the computing resources and all the hosted VCAs as the same impact level (high watermarked) through the PCA definition (everything that can execute simultaneously on the same CPU/memory becomes an 'associated PCA'). If the entity chooses this path, the computing resources are not SCI and this requirement no longer applies. This requirement only applies if the entity chooses to retain differing impact levels of hosted VCAs and isolates them from each other by configuring affinity rules to keep VCAs of differing impact levels from executing on the same underlying hardware resources.

Q11 Comment Theme:

- **Clarity on Requirement 2 and patching cadence for dormant VCAs.**

SDT Response:

Thank you for your comments. The SDT has added more qualifications to the definition of VCA to clarify that a dormant, non-instantiated VM image is not a VCA, and thus not an Applicable System of R2. Other clarifications have been made in CIP-010 to clearly allow for automated vulnerability assessment and remediation of a VCA upon instantiation in a remediation VLAN.

Q11 Comment Theme:

- **Request explicit language in CIP-007 R2 that these patching Requirements do not include patching in the cloud.**

SDT Response: Thank you for your comments. The SDT does not have authorization in its SAR to address the aspects of off-premise cloud computing, of which this is one of numerous issues that would need to be addressed.

Question 12.

The SDT revised CIP-010 based on industry comments. Do you agree with the proposed changes to the NERC Glossary terms? If not, please provide the basis for your disagreement and an alternate proposal.

Q12 Comment Theme:

- **Overall: Changes are not needed/aren't related to virtualization**

SDT Response:

Thank you for your comments. The SDT asserts changes are needed to CIP-010 for virtualization issues. The SDT is making CIP-010 R1 a requirement with a clear change management security objective to alleviate several virtualization-related issues such as how to treat parent/child images (such as in VDI), application containers, clarifying the use of automated vulnerability assessment capability for VMs with remediation VLANs, and inclusion of authorization of change to the security controls affecting VM affinity and network isolation between VMs of differing impact levels.

Previously, CIP-010 R1 was concerned with five prescriptive attributes of a system, several of which caused issues with the virtualization concepts noted above. Rather than continuing to expand a list of prescriptive attributes in R1.1 with a backwards-looking requirement to update a baseline within 30 calendar days after a change is made and in addition determining affected CIP-005 and CIP-007 security controls, the core of the requirement is now the identification and testing of those CIP-005 and CIP-007 security controls and authorization of changes. It now focuses on the security objective of authorizing changes and allows entities to define those changes, taking into account the virtualization issues, that can affect the CIP-005 and CIP-007 security controls.

As an example of a virtualization issue, the SDT considered VDI scenarios where dozens or hundreds of VCAs may be dynamically instantiated from parent images. The SDT's intent is that the goal of R1 is not to maintain perfect baseline configuration of a hundred individual dynamically created VCAs but to focus on the much higher risk of authorizing and thus controlling change to the parent image from which a hundred dynamic images will be created. A forward looking requirement to authorize a change is of more value to reliability than a requirement to update baseline documentation in a certain timeframe after making a change. Another example is dormant VMs that may rarely instantiate. With automated vulnerability assessment and remediation of patches, AV updates, etc. at instantiation, the goal of R1 is not to have the entity somehow track when this automated process happens to each image file and then prove the update of baseline documentation within 30 calendar days. These are two examples of virtualization enabled scenarios where the SDT asserts CIP-010 needs to change to accommodate these advances in technology in a much more dynamic and automated environment. The SDT will incorporate example measures that include baseline configurations as one tool an entity may choose for this requirement.

Q12 Comment Theme:

- **R1/ Part 1.1.1: Add baselines and parent/child (VDI) examples to the measures as clarifying examples**
- **What level of OS change must be authorized?**
- **Why is lack of OS relevant to patching?**
- **The Measure mentions patch 'implementation' vs the requirement for change authorization**

SDT Response: Thank you for your comments. In response to these and numerous other comments on CIP-010 R1 and to allow for scenarios brought about by virtualization, the SDT has chosen to go with an objective level requirement rather than continue to maintain a prescriptive list of system attributes subject to change management processes. This requirement now requires entities to define the types of changes that will be in the change mgt process that includes changes that may impact CIP-005 and CIP-007 controls. Then, for those changes, the requirement focuses on authorizing those changes and the verification that changes do not adversely impact those security controls. This was the core of the previous version's requirement as well, but is now more future-proof and objective oriented.

Q12 Comment Theme:

- **R1/Part 1.1.2: Clarify "application containers"**

SDT Response: Thank you for your comments. The SDT in our draft 1 posting proposed a new glossary term for "Self-Contained Application (SCA)". Most stakeholder comments said that term is unnecessary and to use the IT industry "application container" term instead of proposing a NERC specific definition. The SDT intent for including this phrase is not to create something new but to simply help clarify that "application containers" as understood in the IT industry are to be treated like other application software and not as some unique form of VCA.

Q12 Comment Theme:

- **R1/Part 1.1.4: Ports and services/clarity on dynamic port ranges/tracking ports in the virtualization underlay rather than services/Clarify the authorization for change is to the OS/SW/Config that affects open ports, not every time a port opens/closes.**

SDT Response: Thank you for your comments. The SDT agrees with many of these comments and based on these and others has, in conjunction with changes to CIP-007 R1, made both of these requirements more objective-oriented. This allows these requirements to incorporate virtualization-specific scenarios and modifies the language in such a way that as technology continues to change, these requirements will not require continual update due to maintaining prescriptive lists of system attributes and baseline config documentation of such attributes – including ports and services. As the network accessibility of a system and reducing the network 'attack surface' remains a CIP-007 R1 security objective, then changes to Applicable Systems that can affect this remain the subject of CIP-010 R1 as well.

Q12 Comment Theme:

- **R3/Part 3.3: the requirement to build outside of the production environment and perform the vulnerability scan has been removed**
- **Clarify timeline between the VA and production**
- **Clarify "prior to becoming an Applicable System"**

SDT Response: Thank you for your comments. The SDT asserts the objective to perform a vulnerability assessment of a new Applicable System before it can have an impact in production remains, but has been reworded to allow for virtualization scenarios and automated means of implementing this requirement. The currently approved language states "Prior to adding a new applicable Cyber Asset to a production environment…" which has worked well with the traditional Cyber Asset such as Cyber Assets that arrive on a loading dock. However, it does not work well with a VCA that is created in an isolated environment WITHIN a virtualized infrastructure. It does not arrive from 'outside', it is created in the environment. The SDT changed the language for clarification. The changes should also clarify that automated tools that implement this functionality, such as remediation VLANs, are a good and allowable practice even though it occurs in a production "environment", but not with production network connectivity and the ability to impact other production VCAs.

The SDT's intent is that "prior to becoming an Applicable System" means that prior to the object in question fulfilling the role of one of the Applicable Systems and their definitions. For example, before it can have the 15 minute impact of the BCA definition, or perform the electronic access control function of an ESP or BCS. At the time the object fulfills those roles and thus meets the corresponding definition, that's when it "becomes an Applicable System" of this requirement, and prior to that point in time the vulnerability assessment must have been performed.
The SDT notes that the maximum allowable timeframe between the vulnerability assessment and the production use of the system has not been prescribed to date and is not a virtualization related issue. The SDT is changing the language to clearly allow for automated tools that will perform this task faster and every time a VCA is booted, not just its initial introduction to the environment.

Q12 Comment Theme:

- **R4: TCA scope changes from High/Med and PCAs to "everything but lows" and includes all non-CIP and thus the scoping is entirely in the definitions of TCA/RM**

SDT Response: Thank you for your comments. The SDT agrees and has reinstated updated applicability statements within the CIP-010 R4 requirement language and removed the applicability statements from the previous draft that were in Attachment 1.

Question 13.

The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 (conforming changes) based on industry comments. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

Q13 Comment Theme:

- **CIP-006 R1.10 was moved to CIP-005 R1.4 but the associated PCAs aren't included**

SDT Response: Thank you for your comments. The SDT agrees and has included associated PCA's in the scope of the requirement.

Q13 Comment Theme:

- **CIP-009 should not include SCI in applicability. Recovery of the functionality may occur outside of recovering underlying SCI.**

SDT Response: Thank you for your comments. The SDT agrees that the SCI itself does not always require its own recovery plan. The objective of this requirement is not to recover SCI simply as SCI, but to recover the functionality of the systems it supports that remain in scope. Entities could have recovery plans that recover the functionality in other ways if underlying SCI is the issue. However, entities should be aware that if their plan to recover an Applicable System is dependent upon recovery of the SCI, the SCI should be a part of the documented plan. With the exception of Part 1.5, the SDT removed SCI from the Applicable Systems where it had been included before in Draft 2.

Question 14.

Please provide any additional comments for the SAR drafting team to consider, if desired.

Q14 Comment Theme:

- **Associated Data Center (as required by the latest ERT v5 spreadsheet) is not listed in the draft standard**

SDT Response: Thank you for your comments. The 'associated Data Center' is an included component of the currently approved Control Center definition in the NERC glossary. It is not the subject of any changes by this SDT.

Q14 Comment Theme:

- **Planned and Unplanned changes language should be added to the Implementation Plan, similar to the language included in previous CIP implementation plans.**

SDT Response: Thank you for your comments. The SDT agrees and has copied those sections into the proposed Implementation Plan so those provisions remain with this version.

Q14 Comment Theme:

- **CIP-013 is part of this update, is there a reason why CIP-014 is not part of this update?**

SDT Response: Thank you for your comments. CIP-014 is a physical security standard and is not in the suite of cyber security standards, unlike CIP-006 that is specifically related to the physical security of BES Cyber Systems. While CIP-014 has a few similarities with CIP-002, it is not affected by virtualization technology. CIP-013 on the other hand, is in the suite of Cyber Security standards and is affected by virtualization – such as the procurement of SCI.

REMINDER

Standards Announcement

Project 2016-02 Modifications to CIP Standards

Additional Ballots and Non-binding Polls Open through September 1, 2021

Now Available

The additional ballots and associated Violation Risk Factors and Violation Severity Level non-binding polls for the **CIP Virtualization suite of standards (outlined below)** are open through **8 p.m. Eastern, Wednesday, September 1, 2021**.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-Y - Cyber Security – Security Management Controls
- CIP-004-Y - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-Y - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Balloting
Use the Standards Balloting and Commenting System (SBS) to submit votes.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*

- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual**.**

For more information or assistance, Jordan Mallory (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Applications" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

UPDATED

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Formal Comment Period Extended, Now Open through September 1, 2021

Now Available

Due to numerous requests received from industry, the 45-day formal comment period for the **CIP Virtualization suite of standards (outlined below)** has been extended and is now open through **8 p.m. Eastern, Wednesday, September 1, 2021**.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-Y - Cyber Security – Security Management Controls
- CIP-004-Y - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-Y - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page**.**

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*

- *Please be mindful of ballot and comment period closing dates. We ask to* ***allow at least 48 hours*** *for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts* ***prior to the last day*** *of a comment/ballot period.*

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **August 23 – September 1, 2021**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/229)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 AB 2 ST
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 267
Total Ballot Pool: 303
Quorum: 88.12
Quorum Established Date: 9/1/2021 3:57:33 PM
Weighted Segment Value: 36.32

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	24	0.364	42	0.636	0	8	11
Segment: 2	8	0.8	1	0.1	7	0.7	0	0	0
Segment: 3	66	1	21	0.389	33	0.611	0	6	6
Segment: 4	15	1	6	0.545	5	0.455	0	2	2
Segment: 5	74	1	20	0.364	35	0.636	0	7	12
Segment: 6	46	1	10	0.263	28	0.737	0	3	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	3	0.3	3	0.3	0	1	0
Totals:	303	6.4	85	2.325	153	4.075	0	29	36

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Third-Party Comments
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski	Joseph Knight	Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Negative	Comments Submitted
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Third-Party Comments
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		None	N/A
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		None	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 303 of 303 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/229)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 2 ST
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 267
Total Ballot Pool: 303
Quorum: 88.12
Quorum Established Date: 9/1/2021 4:05:21 PM
Weighted Segment Value: 41.67

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	28	0.424	38	0.576	0	8	11
Segment: 2	8	0.8	2	0.2	6	0.6	0	0	0
Segment: 3	66	1	24	0.444	30	0.556	0	6	6
Segment: 4	15	1	5	0.455	6	0.545	0	2	2
Segment: 5	74	1	23	0.418	32	0.582	0	7	12
Segment: 6	46	1	13	0.342	25	0.658	0	3	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	303	6.2	98	2.584	138	3.616	0	31	36

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		None	N/A
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		None	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 303 of 303 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/229)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 2 ST
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 266
Total Ballot Pool: 301
Quorum: 88.37
Quorum Established Date: 9/1/2021 3:59:04 PM
Weighted Segment Value: 38.21

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	30	0.455	36	0.545	0	8	11
Segment: 2	8	0.8	1	0.1	7	0.7	0	0	0
Segment: 3	66	1	23	0.426	31	0.574	0	6	6
Segment: 4	14	1	5	0.455	6	0.545	0	2	1
Segment: 5	74	1	23	0.418	32	0.582	0	7	12
Segment: 6	45	1	12	0.316	26	0.684	0	2	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	2	0.2	2	0.2	0	3	0
Totals:	301	6.2	96	2.369	140	3.831	0	30	35

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		None	N/A
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		None	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/229)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 2 ST
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 265
Total Ballot Pool: 301
Quorum: 88.04
Quorum Established Date: 9/1/2021 4:02:13 PM
Weighted Segment Value: 20.31

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	9	0.138	56	0.862	0	8	12
Segment: 2	8	0.8	1	0.1	7	0.7	0	0	0
Segment: 3	66	1	8	0.148	46	0.852	0	6	6
Segment: 4	14	1	4	0.364	7	0.636	0	2	1
Segment: 5	74	1	12	0.218	43	0.782	0	7	12
Segment: 6	45	1	5	0.132	33	0.868	0	2	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	2	0.2	4	0.4	0	1	0
Totals:	301	6.4	41	1.3	196	5.1	0	28	36

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Third-Party Comments
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Negative	Comments Submitted
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Negative	Comments Submitted
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Third-Party Comments
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Negative	Comments Submitted
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Third-Party Comments
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		None	N/A
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		None	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Negative	Comments Submitted
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/229)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 AB 2 ST
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 265
Total Ballot Pool: 301
Quorum: 88.04
Quorum Established Date: 9/1/2021 4:02:14 PM
Weighted Segment Value: 42.32

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	29	0.446	36	0.554	0	8	12
Segment: 2	8	0.8	2	0.2	6	0.6	0	0	0
Segment: 3	66	1	24	0.444	30	0.556	0	6	6
Segment: 4	14	1	5	0.455	6	0.545	0	2	1
Segment: 5	74	1	24	0.436	31	0.564	0	7	12
Segment: 6	45	1	13	0.342	25	0.658	0	2	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	301	6.2	100	2.624	135	3.576	0	30	36

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted
3	New York Power Authority	David Rivera		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		None	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Showing 1 to 301 of 301 entries

Previous 1 Next

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/229)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 2 ST
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 265
Total Ballot Pool: 301
Quorum: 88.04
Quorum Established Date: 9/1/2021 4:02:15 PM
Weighted Segment Value: 29.49

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	18	0.281	46	0.719	0	9	12
Segment: 2	8	0.8	1	0.1	7	0.7	0	0	0
Segment: 3	66	1	16	0.296	38	0.704	0	6	6
Segment: 4	14	1	4	0.364	7	0.636	0	2	1
Segment: 5	74	1	18	0.327	37	0.673	0	7	12
Segment: 6	45	1	11	0.289	27	0.711	0	2	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	2	0.2	3	0.3	0	2	0
Totals:	301	6.3	70	1.858	165	4.442	0	30	36

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Third-Party Comments
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Third-Party Comments
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Third-Party Comments
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Abstain	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Third-Party Comments
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Third-Party Comments
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Third-Party Comments
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		None	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/229)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 AB 2 ST
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 266
Total Ballot Pool: 301
Quorum: 88.37
Quorum Established Date: 9/1/2021 4:01:47 PM
Weighted Segment Value: 49.63

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	33	0.5	33	0.5	0	8	11
Segment: 2	8	0.8	3	0.3	5	0.5	0	0	0
Segment: 3	66	1	28	0.519	26	0.481	0	6	6
Segment: 4	14	1	6	0.545	5	0.455	0	2	1
Segment: 5	74	1	28	0.519	26	0.481	0	8	12
Segment: 6	45	1	15	0.395	23	0.605	0	2	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	301	6.2	116	3.077	119	3.123	0	31	35

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Affirmative	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		None	N/A
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/229)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 AB 2 ST
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 266
Total Ballot Pool: 301
Quorum: 88.37
Quorum Established Date: 9/1/2021 4:02:19 PM
Weighted Segment Value: 49.88

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	34	0.515	32	0.485	0	8	11
Segment: 2	8	0.8	3	0.3	5	0.5	0	0	0
Segment: 3	66	1	28	0.519	26	0.481	0	6	6
Segment: 4	14	1	6	0.545	5	0.455	0	2	1
Segment: 5	74	1	28	0.519	26	0.481	0	8	12
Segment: 6	45	1	15	0.395	23	0.605	0	2	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	301	6.2	117	3.092	118	3.108	0	31	35

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Third-Party Comments
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Comments Submitted
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Affirmative	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Third-Party Comments
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		None	N/A
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/229)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 2 ST
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 266
Total Ballot Pool: 301
Quorum: 88.37
Quorum Established Date: 9/1/2021 4:03:06 PM
Weighted Segment Value: 33.32

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	25	0.385	40	0.615	0	9	11
Segment: 2	8	0.8	0	0	8	0.8	0	0	0
Segment: 3	66	1	22	0.407	32	0.593	0	6	6
Segment: 4	14	1	5	0.455	6	0.545	0	2	1
Segment: 5	74	1	20	0.37	34	0.63	0	8	12
Segment: 6	45	1	12	0.316	26	0.684	0	2	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	2	0.2	4	0.4	0	1	0
Totals:	301	6.4	86	2.133	150	4.267	0	30	35

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Third-Party Comments
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Third-Party Comments
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		None	N/A
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted
6	AEP	Justin Kuehne		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		None	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/229)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 AB 2 ST
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 266
Total Ballot Pool: 301
Quorum: 88.37
Quorum Established Date: 9/1/2021 4:03:58 PM
Weighted Segment Value: 40.29

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	28	0.431	37	0.569	0	9	11
Segment: 2	8	0.8	1	0.1	7	0.7	0	0	0
Segment: 3	66	1	24	0.444	30	0.556	0	6	6
Segment: 4	14	1	5	0.455	6	0.545	0	2	1
Segment: 5	74	1	23	0.426	31	0.574	0	8	12
Segment: 6	45	1	13	0.342	25	0.658	0	2	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	301	6.2	97	2.498	137	3.702	0	32	35

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr.		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		None	N/A
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		None	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/229)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 AB 2 ST
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 266
Total Ballot Pool: 301
Quorum: 88.37
Quorum Established Date: 9/1/2021 4:04:42 PM
Weighted Segment Value: 41.56

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	29	0.446	36	0.554	0	9	11
Segment: 2	8	0.8	1	0.1	7	0.7	0	0	0
Segment: 3	66	1	25	0.463	29	0.537	0	6	6
Segment: 4	14	1	5	0.455	6	0.545	0	2	1
Segment: 5	74	1	24	0.444	30	0.556	0	8	12
Segment: 6	45	1	14	0.368	24	0.632	0	2	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	301	6.2	101	2.577	133	3.623	0	32	35

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Third-Party Comments
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Third-Party Comments
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		None	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Third-Party Comments
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Third-Party Comments
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
1	Xcel Energy, Inc.	Dean Schiro		Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Patrick Woods		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Third-Party Comments
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Negative	Third-Party Comments
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Third-Party Comments
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Third-Party Comments
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Negative	Comments Submitted
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Muscatine Power and Water	Neal Nelson		Negative	Third-Party Comments
5	National Grid USA	Robin Berry		None	N/A
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PSEG - PSEG Fossil LLC	Tim Kucey		Negative	Third-Party Comments
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Negative	Comments Submitted
6	AEP	Justin Kuehne		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Manitoba Hydro	Kelly Bertholet		None	N/A
6	Muscatine Power and Water	Nicholas Burns		Negative	Third-Party Comments
6	New York Power Authority	Erick Barrios		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Comments Submitted
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 | Non-binding Poll AB 2 NB
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 243
Total Ballot Pool: 277
Quorum: 87.73
Quorum Established Date: 9/1/2021 4:05:27 PM
Weighted Segment Value: 37.36

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	78	1	20	0.392	31	0.608	16	11
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	63	1	17	0.395	26	0.605	13	7
Segment: 4	14	0.9	5	0.5	4	0.4	4	1
Segment: 5	65	1	15	0.357	27	0.643	15	8
Segment: 6	41	1	7	0.25	21	0.75	7	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	3	0.3	1	0.1	3	0
Totals:	277	5.8	68	2.295	114	3.505	61	34

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Negative	Comments Submitted
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Rachel Schuldt		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 277 of 277 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 | Non-binding Poll AB 2 NB
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 244
Total Ballot Pool: 277
Quorum: 88.09
Quorum Established Date: 9/1/2021 4:04:05 PM
Weighted Segment Value: 43.96

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	78	1	24	0.462	28	0.538	16	10
Segment: 2	8	0.5	2	0.2	3	0.3	2	1
Segment: 3	63	1	19	0.442	24	0.558	13	7
Segment: 4	14	0.9	5	0.5	4	0.4	4	1
Segment: 5	65	1	17	0.405	25	0.595	15	8
Segment: 6	41	1	10	0.357	18	0.643	7	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	3	0.3	0	0	4	0
Totals:	277	5.7	80	2.665	102	3.035	62	33

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Negative	Comments Submitted
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Showing 1 to 277 of 277 entries

Previous 1 Next

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 | Non-binding Poll AB 2 NB
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 244
Total Ballot Pool: 277
Quorum: 88.09
Quorum Established Date: 9/1/2021 4:04:20 PM
Weighted Segment Value: 44.81

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	78	1	26	0.491	27	0.509	15	10
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	63	1	20	0.465	23	0.535	13	7
Segment: 4	14	0.9	5	0.5	4	0.4	4	1
Segment: 5	65	1	18	0.429	24	0.571	15	8
Segment: 6	41	1	10	0.357	18	0.643	7	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	2	0.2	1	0.1	4	0
Totals:	277	5.7	82	2.541	101	3.159	61	33

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 277 of 277 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 | Non-binding Poll AB 2 NB
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 244
Total Ballot Pool: 277
Quorum: 88.09
Quorum Established Date: 9/1/2021 4:04:37 PM
Weighted Segment Value: 19.67

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	78	1	9	0.173	43	0.827	16	10
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	63	1	6	0.14	37	0.86	13	7
Segment: 4	14	0.9	4	0.4	5	0.5	4	1
Segment: 5	65	1	10	0.238	32	0.762	15	8
Segment: 6	41	1	4	0.143	24	0.857	7	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	277	5.8	36	1.394	147	4.406	61	33

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Josh Combs		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Negative	Comments Submitted
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Negative	Comments Submitted
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 277 of 277 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 | Non-binding Poll AB 2 NB
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 245
Total Ballot Pool: 278
Quorum: 88.13
Quorum Established Date: 9/1/2021 4:04:54 PM
Weighted Segment Value: 45.6

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	25	0.481	27	0.519	17	10
Segment: 2	8	0.5	2	0.2	3	0.3	2	1
Segment: 3	63	1	20	0.465	23	0.535	13	7
Segment: 4	14	0.9	5	0.5	4	0.4	4	1
Segment: 5	65	1	18	0.429	24	0.571	15	8
Segment: 6	41	1	10	0.357	18	0.643	7	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	3	0.3	0	0	4	0
Totals:	278	5.7	83	2.732	99	2.968	63	33

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Comments Submitted
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 | Non-binding Poll AB 2 NB
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 244
Total Ballot Pool: 278
Quorum: 87.77
Quorum Established Date: 9/1/2021 4:09:58 PM
Weighted Segment Value: 28.02

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	13	0.255	38	0.745	17	11
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	63	1	11	0.256	32	0.744	13	7
Segment: 4	14	0.9	4	0.4	5	0.5	4	1
Segment: 5	65	1	13	0.31	29	0.69	15	8
Segment: 6	41	1	7	0.25	21	0.75	7	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	278	5.8	51	1.77	131	4.03	62	34

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Comments Submitted
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Abstain	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Negative	Comments Submitted
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 | Non-binding Poll AB 2 NB
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 245
Total Ballot Pool: 278
Quorum: 88.13
Quorum Established Date: 9/1/2021 4:05:41 PM
Weighted Segment Value: 52.46

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	28	0.538	24	0.462	17	10
Segment: 2	8	0.5	2	0.2	3	0.3	2	1
Segment: 3	63	1	24	0.545	20	0.455	12	7
Segment: 4	14	0.9	5	0.5	4	0.4	4	1
Segment: 5	65	1	22	0.524	20	0.476	15	8
Segment: 6	41	1	12	0.429	16	0.571	7	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	3	0.3	0	0	4	0
Totals:	278	5.7	96	3.036	87	2.664	62	33

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Comments Submitted
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Affirmative	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 | Non-binding Poll AB 2 NB
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 244
Total Ballot Pool: 278
Quorum: 87.77
Quorum Established Date: 9/1/2021 4:11:24 PM
Weighted Segment Value: 53.3

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	29	0.558	23	0.442	16	11
Segment: 2	8	0.5	2	0.2	3	0.3	2	1
Segment: 3	63	1	24	0.558	19	0.442	13	7
Segment: 4	14	0.9	5	0.5	4	0.4	4	1
Segment: 5	65	1	22	0.524	20	0.476	15	8
Segment: 6	41	1	12	0.429	16	0.571	7	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	3	0.3	0	0	4	0
Totals:	278	5.7	97	3.068	85	2.632	62	34

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Comments Submitted
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Affirmative	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Affirmative	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Affirmative	N/A
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 | Non-binding Poll AB 2 NB
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 245
Total Ballot Pool: 278
Quorum: 88.13
Quorum Established Date: 9/1/2021 4:06:13 PM
Weighted Segment Value: 36.07

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	19	0.373	32	0.627	17	11
Segment: 2	8	0.6	1	0.1	5	0.5	2	0
Segment: 3	63	1	17	0.395	26	0.605	13	7
Segment: 4	14	0.9	5	0.5	4	0.4	4	1
Segment: 5	65	1	14	0.333	28	0.667	15	8
Segment: 6	41	1	8	0.286	20	0.714	7	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	278	5.9	66	2.187	117	3.713	62	33

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Negative	Comments Submitted
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Negative	Comments Submitted
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Comments Submitted
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Negative	Comments Submitted
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Negative	Comments Submitted
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Negative	Comments Submitted
6	Austin Energy	Lisa Martin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 | Non-binding Poll AB 2 NB
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 243
Total Ballot Pool: 277
Quorum: 87.73
Quorum Established Date: 9/1/2021 4:12:56 PM
Weighted Segment Value: 45

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	78	1	24	0.48	26	0.52	17	11
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	63	1	20	0.465	23	0.535	13	7
Segment: 4	14	0.9	5	0.5	4	0.4	4	1
Segment: 5	65	1	18	0.429	24	0.571	15	8
Segment: 6	41	1	10	0.357	18	0.643	7	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	3	0.3	0	0	4	0
Totals:	277	5.7	81	2.631	99	3.069	63	34

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Comments Submitted
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 277 of 277 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 | Non-binding Poll AB 2 NB
Voting Start Date: 8/23/2021 12:01:00 AM
Voting End Date: 9/1/2021 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 243
Total Ballot Pool: 278
Quorum: 87.41
Quorum Established Date: 9/1/2021 4:13:20 PM
Weighted Segment Value: 45.56

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	24	0.471	27	0.529	17	11
Segment: 2	8	0.5	1	0.1	4	0.4	2	1
Segment: 3	63	1	20	0.476	22	0.524	13	8
Segment: 4	14	0.9	5	0.5	4	0.4	4	1
Segment: 5	65	1	18	0.429	24	0.571	15	8
Segment: 6	41	1	11	0.393	17	0.607	7	6
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	3	0.3	0	0	4	0
Totals:	278	5.7	82	2.668	98	3.032	63	35

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Abstain	N/A
1	Balancing Authority of Northern California	Kevin Smith		Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Frank Pace		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Negative	Comments Submitted
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Abstain	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Evergy	Allen Klassen		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch	Joseph Knight	Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Abstain	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Nurul Abser		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Negative	Comments Submitted
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Kyle Hussey		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao		Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Bret Galbraith		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Jamie Johnson		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Brandon Gleason		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Negative	Comments Submitted
3	Eversource Energy	Christopher McKinnon		Negative	Comments Submitted
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Negative	Comments Submitted
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Affirmative	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Dan Zollner		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney		Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Jeremy Lorigan		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua		Negative	Comments Submitted
4	Seattle City Light	Hao Li		Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Brad Haralson		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury	Casey Jones	Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Abstain	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Comments Submitted
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		Abstain	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Constellation	Alison MacKellar		None	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Abstain	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		None	N/A
5	Evergy	Derek Brown		Negative	Comments Submitted
5	Exelon	Cynthia Lee		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Becky Rinier		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Los Angeles Department of Water and Power	Glenn Barry		Affirmative	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Anthony Stevens		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		Negative	Comments Submitted
5	NB Power Corporation	Rob Vance		Negative	Comments Submitted
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu	David Kwan	Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi		Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seattle City Light	Faz Kasraie		Abstain	N/A
5	Seminole Electric Cooperative, Inc.	Trena Haynes		Abstain	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		None	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Cristhian Godoy		Negative	Comments Submitted
6	Constellation	Kimberly Turco		None	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Evergy	Thomas ROBBEN		Negative	Comments Submitted
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Corporation	Ann Carey		Affirmative	N/A
6	Great River Energy	Donna Stephenson	Joseph Knight	Negative	Comments Submitted
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	New York Power Authority	Erick Barrios		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Sing Tay		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton		Affirmative	N/A
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Seattle City Light	Brian Belger		None	N/A
6	Snohomish County PUD No. 1	John Liang		Negative	Comments Submitted
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	David Hathaway		Negative	Comments Submitted
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Showing 1 to 278 of 278 entries

Previous 1 Next

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the Bulk Electric System (BES). Identification and categorization of BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-7:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan"

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of Parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** RAS that support the reliable operation of the Bulk Electric System; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #			Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1			For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer of identified BCS have not been categorized or have been incorrectly categorized at a lower category;	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent but less than or equal to 10	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BCS, more than 10 percent but less than or equal to 15 percent of	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category;

R #			Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or fewer identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or fewer high or medium BCS have not been identified.	percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BCS, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent but less than or equal to 10 percent high or medium BCS have not been identified; OR	identified BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BCS, more than 10 but less than or equal to 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 10 percent but less than or equal to 15 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or	OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of high or medium impact BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BCS have not been identified.

R #			Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than five but less than or equal to 10 high or medium BCS have not been identified.	fewer high and medium impact BCS, more than 10 but less than or equal to 15 high or medium BCS have not been identified.	
R2			The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (Part2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (Part 2.2)

R #			Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than or equal to 16 calendar months of the previous approval. (Part 2.2)	less than or equal to 17 calendar months of the previous approval. (Part 2.2)	less than or equal to 18 calendar months of the previous approval. (Part 2.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High impact rating**
   Each BCS used by and located at any of the following:

   1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

   1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

   1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

   1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium impact rating**
   Each BCS, not included in Section 1 above, associated with any of the following:

   2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

   2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

   2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

   2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each RAS or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in high impact rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in high impact rating, above.

2.13. Each Control Center or backup Control Center, not already included in High impact rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low impact rating

BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. RAS that support the reliable operation of the Bulk Electric System.

For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
~~45~~63-day formal comment period with ballot	June 30 – ~~August 13~~September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~May 11 – June 24, 2021~~
~~45-day formal comment period with ballot~~	~~August 29–October 11, 2021~~
Final Ballot	~~October 19–28, 2021~~April 2022
Board adoption	~~November 4, 2021~~May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 3 Definitions"

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization
2. **Number:** CIP-002-7
3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the Bulk Electric System (BES). Identification and categorization of BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.
4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-7:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication network and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** RAS that support the reliable operation of the ~~Bulk Electric System~~BES; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. ~~Per Attachment 1, Section 1, i~~Identify each ~~BES Cyber System~~BCS ~~as either of the following~~according to Attachment 1, Section 1, if any, at each asset;

- ~~A high impact BCS including any supporting SCI as part of the BCS; or~~
- ~~A high impact BCS and independent SCI supporting any part of the high impact BCS or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).~~

~~**1.4.**~~**1.2.** ~~Per Attachment 1, Section 2, i~~Identify each medium impact ~~BES Cyber System~~BCS ~~as either of the~~ according to Attachment 1, Section 2, following, if any, at each asset;

- ~~A medium impact BCS including any supporting SCI as part of the BCS; or~~
- ~~A medium impact BCS and independent SCI supporting any part of the medium impact BES Cyber System or its associated EACMS, PACS or PCAs.~~

~~**1.5.**~~**1.3.** ~~Per Attachment 1, Section 3, i~~Identify ~~any~~ each asset that contains a low impact BCS~~, or SCI that supports any part of a low impact BCS~~ according to Attachment 1, Section 3, if any (a discrete list of low impact BCS or SCI that supports any part of a low impact BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. **Compliance Monitoring Process:**

    1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

    1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

    The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

    - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
    - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
    - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

    1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS~~ or independently identified SCI~~, five percent or fewer of identified BCS ~~or independently identified SCI,~~ have not been categorized or have been incorrectly categorized at a lower category; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS~~ or independently identified SCI~~, more than five percent but less than or equal to 10 percent of identified BCS~~ or independently identified~~	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BCS ~~or independently identified SCI~~, more than 10 percent but less than or equal to 15 percent of identified BCS~~ or independently identified SCI~~, have not been categorized	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 15 percent of identified BCS~~ or independently identified SCI,~~ have not been categorized or have been incorrectly categorized at a lower category;

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	For Responsible Entities with a total of 100 or fewer high and medium impact BCS ~~or independently identified SCI~~, five or fewer identified BCS ~~or independently identified SCI~~ have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS ~~or independently identified SCI~~, five percent or fewer high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS ~~or independently identified SCI~~, five or fewer high or medium BCS ~~or independently identified SCI~~, have not been identified.	~~SCI~~, have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BCS ~~or independently identified SCI~~, have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS ~~or independently identified SCI~~, more than five percent but less than or equal to 10 percent high or medium BCS ~~or independently identified SCI~~, have not been identified;	or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BCS~~A~~, more than 10 but less than or equal to 15 identified BCS~~A~~ have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS ~~or independently identified SCI~~, more than 10 percent but less than or equal to 15 percent high or medium BCS ~~or independently identified SCI~~, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS ~~or independently identified SCI~~,	OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS ~~or independently identified SCI~~, more than 15 identified BCS ~~or independently identified SCI~~ have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS ~~or independently identified SCI~~, more than 15 percent of high or medium impact BCS ~~or independently identified SCI~~, have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS ~~or independently identified SCI~~, more than 15 high or medium impact BCS ~~or~~

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS ~~or independently identified SCI~~, more than five but less than or equal to 10 high or medium BCS ~~or independently identified SCI~~, have not been identified.	more than 10 but less than or equal to 15 high or medium BCS ~~or independently identified SCI~~, have not been identified.	~~independently identified SCI~~, have not been identified.
R2	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (~~Requirement R2~~ Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (~~R~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (~~R~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (~~Requirement R2~~ Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (~~Requirement R2~~ Part 2.2)

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous approval. (~~Requirement R2~~ Part 2.2)	months but less than or equal to 17 calendar months of the previous approval. (~~Requirement R2~~ Part 2.2)	months of the previous approval. (~~Requirement R2~~ Part 2.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Modification to CIP Standards Implementation plan”.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced "Devices" with "Systems" in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6		Criteria 2.12 Modifications Withdrawn	
7		Virtualization modifications.	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High ~~I~~impact ~~R~~rating**

   Each BCS used by and located at any of the following:

   1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

   1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

   1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

   1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium ~~I~~impact ~~R~~rating**

   Each BCS, not included in Section 1 above, associated with any of the following:

~~Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are:~~

~~Each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection; or~~

   2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

   ~~2. Any SCI (which must be included in a shared BCS) supporting one or more BCS that together could, within 15 minutes, adversely impact the reliable operation of any~~

~~combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). ~~-~~The only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each RAS or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating, above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low ~~I~~impact ~~R~~rating

BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. RAS that support the reliable operation of the BES.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7~~5.1a~~

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those ~~BES Cyber Systems~~BCS could have on the reliable operation of the Bulk Electric System (BES). Identification and categorization of ~~BES Cyber Systems~~BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and

including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

~~4.1.6.~~4.1.5. Reliability Coordinator

~~4.1.7.~~4.1.6. Transmission Operator

~~4.1.8.~~4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~Special Protection System or Remedial Action Scheme~~RAS where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-7~~5.1a~~:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~**4.2.3.2.**~~**4.2.3.3.** Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan"

~~1. **24 Months Minimum** – CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

~~**6. Background:**~~

~~This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.~~

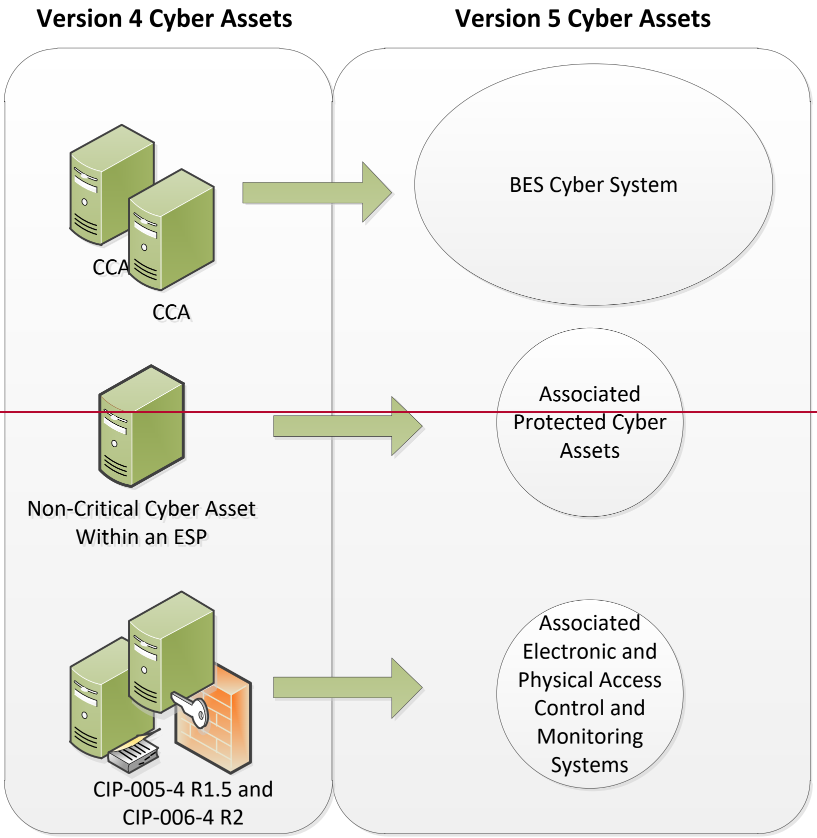
~~Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW~~

~~represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~BES Cyber Systems~~

~~One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.~~



~~In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.~~

~~Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and~~

~~compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.~~

~~It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Reliable Operation of the BES~~

~~The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.~~

~~Real-time Operations~~

~~One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.~~

~~Categorization Criteria~~

~~The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.~~

~~This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.~~

~~Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems~~

~~BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:~~

~~Electronic Access Control or Monitoring Systems (“EACMS”) –~~ ~~Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.~~

~~Physical Access Control Systems (“PACS”)–~~ ~~Examples include: authentication servers, card systems, and badge control systems.~~

~~Protected Cyber Assets (“PCA”) –~~ ~~Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of ~~p~~Parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. ~~Special Protection Systems~~RAS that support the reliable operation of the ~~Bulk Electric System~~BES; and
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact ~~BES Cyber Systems~~BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact ~~BES Cyber Systems~~BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact ~~BES Cyber System~~BCS according to Attachment 1, Section 3, if any (a discrete list of low impact ~~BES Cyber Systems~~BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1~~, and Parts 1.1 and 1.2~~.

R2. ~~The~~ Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

“Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions. ~~The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Assessment~~ Enforcement ~~Processes~~Program:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~

- ~~Complaint~~

~~7.0. Additional Compliance Information~~

- ~~None~~**~~Table of Compliance Elements~~**

Violation Severity Levels

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	~~Operations Planning~~	~~High~~	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Systems~~BCS, five percent or fewer of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, five or fewer identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium	For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than five percent but less than or equal to 10 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and ~~BES Cyber Systems~~BCS, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 high or medium impact ~~BES Cyber Systems~~BCS, more than 10 percent but less than or equal to 15 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and ~~BES Cyber Assets~~BCS, more than 10 but less than or equal to 15 identified ~~BES Cyber Assets~~BCS have not been categorized or have been incorrectly	~~Systems~~BCS, more than 15 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than 15 identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			impact ~~BES Cyber Systems~~BCS, five percent or fewer high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, five or fewer high or medium ~~BES Cyber Systems~~BCS have not been identified.	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than five percent but less than or equal to 10 percent high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than five but less than or equal to 10 high or medium ~~BES Cyber Systems~~BCS	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 10 percent but less than or equal to 15 percent high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than 10 but less than or equal to 15 high or medium ~~BES Cyber Systems~~BCS	impact ~~BES Cyber Systems~~BCS, more than 15 percent of high or medium impact ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact ~~BES Cyber Systems~~BCS have not been identified.

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				have not been identified.	have not been identified.	
R2	~~Operations Planning~~	~~Lower~~	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (~~R~~Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (~~R~~Part2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (~~R~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (~~R~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (~~R~~Part 2.2)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the previous approval. (~~R~~Part 2.2)	of the previous approval. (~~R~~Part 2.2)	of the previous approval. (~~R~~Part 2.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

~~CIP-002-5.1a - Attachment 1~~

~~Impact Rating Criteria~~

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High i~~I~~mpact r~~R~~ating ~~(H)~~**
   Each ~~BES Cyber System~~BCS used by and located at any of the following:

   1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

   1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

   1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

   1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium i~~I~~mpact r~~R~~ating ~~(M)~~**
   Each ~~BES Cyber System~~BCS, not included in Section 1 above, associated with any of the following:

   2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

   2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~ each discrete shared ~~BES Cyber Systems~~ BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each ~~Special Protection System (SPS), Remedial Action Scheme (~~RAS~~),~~ or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in h~~H~~igh i~~I~~mpact r~~R~~ating ~~(H)~~ above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in h~~H~~igh i~~I~~mpact r~~R~~ating ~~(H)~~, above.

2.13. Each Control Center or backup Control Center, not already included in High i~~I~~mpact r~~R~~ating ~~(H)~~ above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low i~~I~~mpact r~~R~~ating ~~(L)~~

~~BES Cyber Systems~~BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. ~~Special Protection Systems~~RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.~~

~~For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.~~

~~CIP-002-5.1a~~

~~CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, “…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES.”~~

~~The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber~~

~~Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:~~

~~Dynamic Response to BES conditions~~
~~Balancing Load and Generation~~
~~Controlling Frequency (Real Power)~~
~~Controlling Voltage (Reactive Power)~~
~~Managing Constraints~~
~~Monitoring & Control~~
~~Restoration of BES~~
~~Situational Awareness~~
~~Inter-Entity Real-Time Coordination and Communication~~

~~Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.~~

~~**Entity Registration**~~	~~**RC**~~	~~**BA**~~	~~**TOP**~~	~~**TO**~~	~~**DP**~~	~~**GOP**~~	~~**GO**~~
~~Dynamic Response~~		~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Balancing Load & Generation~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Controlling Frequency~~		~~X~~				~~X~~	~~X~~
~~Controlling Voltage~~			~~X~~	~~X~~	~~X~~		~~X~~
~~Managing Constraints~~	~~X~~		~~X~~			~~X~~	
~~Monitoring and Control~~			~~X~~			~~X~~	
~~Restoration~~			~~X~~			~~X~~	
~~Situation Awareness~~	~~X~~	~~X~~	~~X~~			~~X~~	
~~Inter-Entity coordination~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~	~~X~~

~~Dynamic Response~~

~~The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:~~

- ~~Spinning reserves (contingency reserves)~~
    - ~~Providing actual reserve generation when called upon (GO,GOP)~~
    - ~~Monitoring that reserves are sufficient (BA)~~
- ~~Governor Response~~
    - ~~Control system used to actuate governor response (GO)~~
- ~~Protection Systems (transmission & generation)~~
    - ~~Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)~~
    - ~~Zone protection for breaker failure (DP, TO, TOP)~~
    - ~~Breaker protection (DP, TO, TOP)~~
    - ~~Current, frequency, speed, phase (TO,TOP, GO,GOP)~~
- ~~Special Protection Systems or Remedial Action Schemes~~
    - ~~Sensors, relays, and breakers, possibly software (DP, TO, TOP)~~
- ~~Under and Over Frequency relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Under and Over Voltage relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Power System Stabilizers (GO)~~

~~Balancing Load and Generation~~

~~The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:~~

- ~~Calculation of Area Control Error (ACE)~~
    - ~~Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)~~
    - ~~Software used to perform calculation (BA)~~
- ~~Demand Response~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP,DP)~~
- ~~Manually Initiated Load shedding~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP, DP)~~

- ~~Non-spinning reserve (contingency reserve)~~
    - ~~Know generation status, capability, ramp rate, start time (GO, BA)~~
    - ~~Start units and provide energy (GOP)~~

~~Controlling Frequency (Real Power)~~

~~The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:~~

- ~~Generation Control (such as AGC)~~
    - ~~ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)~~
    - ~~Software to calculate unit adjustments (BA)~~
    - ~~Transmit adjustments to individual units (GOP)~~
    - ~~Unit controls implementing adjustments (GOP)~~
- ~~Regulation (regulating reserves)~~
    - ~~Frequency source, schedule (BA)~~
    - ~~Governor control system (GO)~~

~~Controlling Voltage (Reactive Power)~~

~~The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:~~

- ~~Automatic Voltage Regulation (AVR)~~
    - ~~Sensors, stator control system, feedback (GO)~~
- ~~Capacitive resources~~
    - ~~Status, control (manual or auto), feedback (TOP, TO,DP)~~
- ~~Inductive resources (transformer tap changer, or inductors)~~
    - ~~Status, control (manual or auto), feedback (TOP,TO,DP)~~
- ~~Static VAR Compensators (SVC)~~
    - ~~Status, computations, control (manual or auto), feedback (TOP, TO,DP)~~

~~Managing Constraints~~

~~Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:~~

- ~~Available Transfer Capability (ATC) (TOP)~~
- ~~Interchange schedules (TOP, RC)~~
- ~~Generation re-dispatch and unit commit (GOP)~~
- ~~Identify and monitor SOL's & IROL's (TOP, RC)~~
- ~~Identify and monitor Flow gates (TOP, RC)~~

~~Monitoring and Control~~

~~Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:~~

- ~~All methods of operating breakers and switches~~
  - ~~SCADA (TOP, GOP)~~
  - ~~Substation automation (TOP)~~

~~Restoration of BES~~

~~The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:~~

- ~~Restoration including planned cranking path~~
  - ~~Through black start units (TOP, GOP)~~
  - ~~Through tie lines (TOP, GOP)~~
- ~~Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)~~
- ~~Coordination (TOP, TO, BA, RC, DP, GO, GOP)~~

~~Situational Awareness~~

~~The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:~~

- ~~Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)~~
- ~~Change management (TOP,GOP,RC,BA)~~
- ~~Current Day and Next Day planning (TOP)~~
- ~~Contingency Analysis (RC)~~
- ~~Frequency monitoring (BA, RC)~~

~~Inter-Entity Coordination~~

~~The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:~~

- ~~Scheduled interchange (BA,TOP,GOP,RC)~~
- ~~Facility operational data and status (TO, TOP, GO, GOP, RC, BA)~~
- ~~Operational directives (TOP, RC, BA)~~

~~Applicability to Distribution Providers~~

~~It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.~~

~~Requirement R1:~~

~~Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.~~

~~Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.~~

~~Attachment 1~~

~~Overall Application~~

~~In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.~~

- ~~When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.~~
- ~~In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.~~
- ~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.~~

~~High Impact Rating (H)~~

~~This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some~~

~~of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.~~

~~The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.~~

~~Additional thresholds as specified in the criteria apply for this category.~~

~~Medium Impact Rating (M)~~

~~Generation~~

~~The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.~~

- ~~Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.~~

  ~~In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.~~

  ~~By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.~~

~~The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.~~

- ~~In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.~~

  ~~If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.~~

  ~~The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.~~

- ~~Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~

  ~~IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.~~

- ~~Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.~~

- ~~Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.~~

- ~~Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Transmission~~

~~The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.~~

- ~~Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.~~

- ~~Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.~~

~~It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.~~

- ~~Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:~~
    - ~~Excluded radial facilities that would only provide support for single generation facilities.~~
    - ~~Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.~~

~~The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.~~

~~Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:~~

- ~~230 kV –> 700 MVA~~
- ~~345 kV –> 1,300 MVA~~
- ~~500 kV –> 2,000 MVA~~
- ~~765 kV –> 3,000 MVA~~

~~In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:~~

- ~~For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate~~

~~connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.~~

  - ~~Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~

  - ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

~~Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.~~

1. ~~The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.~~
2. ~~The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.~~

~~The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.~~

- ~~Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~

- ~~Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.~~

- ~~Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.~~

- ~~Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.~~

- ~~Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.~~

  ~~This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.~~

~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.~~

- ~~Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.~~
- ~~Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Low Impact Rating (L)~~

~~BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.~~

~~Restoration Facilities~~

- ~~Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.~~

  ~~In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.~~

  ~~The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.~~

~~Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.~~

~~BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~

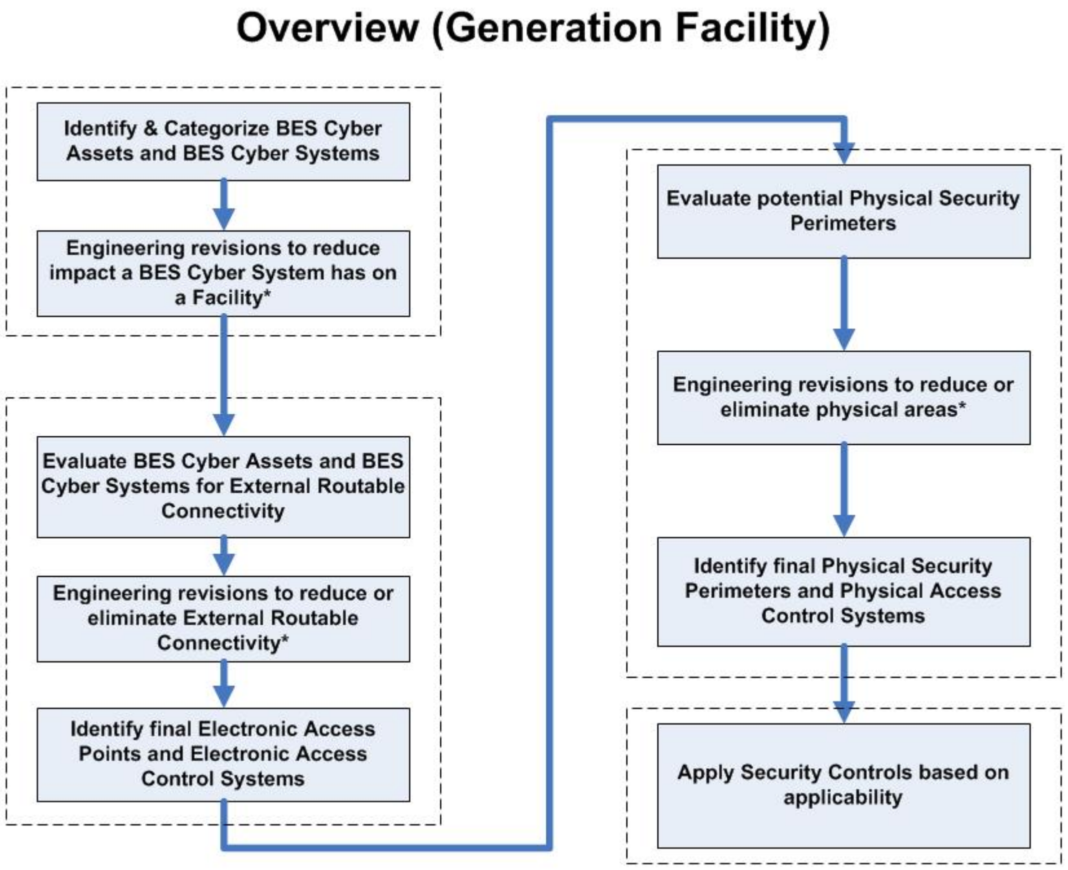
~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.~~

~~Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.~~

~~Use Case: CIP Process Flow~~

~~The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.~~



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for R1:~~

~~BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of “bright-line” criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~Rationale for R2:~~

~~The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager’s approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.~~

~~Appendix 1~~

~~**Requirement Number and Text of Requirement**~~
~~CIP-002-5.1, Requirement R1~~ ~~R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:~~ ~~Control Centers and backup Control Centers;~~ ~~Transmission stations and substations;~~ ~~Generation resources;~~ ~~Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;~~ ~~Special Protection Systems that support the reliable operation of the Bulk Electric System; and~~ ~~For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.~~ ~~Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;~~ ~~Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and~~ ~~Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).~~ ~~Attachment 1, Criterion 2.1~~ ~~Medium Impact Rating (M)~~ ~~Each BES Cyber System, not included in Section 1 above, associated with any of the following:~~ ~~Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~
~~**Questions**~~
~~Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."~~ ~~The Interpretation Drafting Team identified the following questions in the RFI:~~

~~Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~ ~~Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~ ~~If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~
~~Responses~~
~~Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~ ~~The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)~~ ~~Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:~~ ~~The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~ **~~Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~** ~~The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.~~ ~~The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:~~ ~~Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1~~

~~and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1:~~ **~~Impact Rating of Generation Resource Shared BES Cyber Systems~~** ~~for further information and examples.~~

~~Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~The phrase applies to each discrete BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-Y

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1. **Balancing Authority**

      4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

            4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

      4.1.3. **Generator Operator**

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-Y:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links, between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports any part of a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority:** “Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1			The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of

<table>
<tr><th rowspan="2">R #</th><th rowspan="2"></th><th rowspan="2"></th><th colspan="4">Violation Severity Levels (CIP-003-Y)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td>cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1)
OR
The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the six topics required by Requirement R1. (Part 1.2)
OR
The Responsible Entity did not complete its review of the one or</td><td>more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1)
OR
The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the six topics required by R1. (Part 1.2)
OR
The Responsible Entity did not complete its review of the one or</td><td>Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1)
OR
The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the six topics required by Requirement R1. (Part 1.2)
OR
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in</td><td>the previous review. (Requirement R1)
OR
The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1)
OR
The Responsible Entity did not address four or more of the six topics required by Requirement R1. (Part 1.2)
OR
The Responsible Entity did not have any</td></tr>
</table>

<table>
<tr><th rowspan="2">R #</th><th rowspan="2"></th><th rowspan="2"></th><th colspan="4">Violation Severity Levels (CIP-003-Y)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td>more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.2)
OR
The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of</td><td>more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2)
OR
The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to</td><td>less than or equal to 18 calendar months of the previous review. (Part 1.2)
OR
The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)</td><td>documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by R1. (R1.2)
OR
The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)</td></tr>
</table>

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (Part 1.2)	17 calendar months of the previous approval. (Part 1.2)		
R2			The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2,	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2,	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2,	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BCS according to Requirement R2, Attachment 1. (Requirement R2)

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 4. (R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	Attachment 1, Section 3. (R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity that provides access to low impact BCS(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR	Attachment 1, Section 4. (R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party	

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2)	other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3			The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change in less than 40 calendar days of the change. (Requirement R3)	change in less than 50 calendar days of the change. (Requirement R3)	calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4			The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports any part of a low BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports any part of low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports any part of a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports any part of a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TTCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports any part of a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports any part of a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications between Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process

documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, controls to maintain the known good state of the OS and software, application whitelisting practices, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of controls to maintain the known good state of the OS and software, or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the

party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~second~~ third draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – August 13, 2021
45-day form comment period with ballot	February 4 – March 21, 2022

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~August 29–October 11, 2021~~
Final Ballot	~~October 19–28, 2021~~ April 2022
Board adoption	~~November 4, 2021~~May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-Y

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-Y:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links~~ logically isolated from, but not providing logical isolation for, BCS or Shared Cyber Infrastructure (SCI)~~ between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ~~Electronic Security Perimeter (~~ESP~~)~~ that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1.** For its high impact and medium impact BCS, if any:
  - **1.1.1.** Personnel and training (CIP-004);
  - **1.1.2.** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
  - **1.1.3.** Physical security of BCS (CIP-006);
  - **1.1.4.** System security management (CIP-007);
  - **1.1.5.** Incident reporting and response planning (CIP-008);
  - **1.1.6.** Recovery plans for BCS (CIP-009);
  - **1.1.7.** Configuration change management and vulnerability assessments (CIP-010);
  - **1.1.8.** Information protection (CIP-011); and
  - **1.1.9.** Declaring and responding to CIP Exceptional Circumstances.
- **1.2.** For its assets identified in CIP-002 containing low impact BCS, if any:
  - **1.2.1.** Cyber security awareness;
  - **1.2.2.** Physical security controls;
  - **1.2.3.** Electronic access controls;
  - **1.2.4.** Cyber Security Incident response;
  - **1.2.5.** Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and
  - **1.2.6.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports any part of a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS ~~or SCI that supports any part of a low impact BCS~~ or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	~~Operations Planning~~	~~Medium~~	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BCS but~~ did not address one of the nine topics required by Requirement R1. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BCS but~~ did not address two of the nine topics required by Requirement R1. (~~Requirement R1~~ Part R1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BCS but~~ did not address three of the nine topics required by Requirement R1. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BCS but~~ did not address four or more of the nine topics required by Requirement R1. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (~~Requirement R1~~ Part 1.1)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months but did complete this review in less than or equal to 16 calendar months of the previous review. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17	calendar months of the previous review. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 18

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity ~~documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS but~~ did not address one of the six topics required by Requirement R1. (~~Requirement R1~~ Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified	calendar months of the previous approval. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity documented one or ~~more cyber security policies for its assets identified in CIP-002 containing low impact BCS but~~ did not address two of the six topics required by Requirement R1. (~~Requirement R1~~ Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for	identified in CIP-002 containing low impact BCS but did not address three of the six topics required by Requirement R1. (~~Requirement R1~~ Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (~~Requirement R1~~ Part 1.2) OR	calendar months of the previous approval. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity ~~documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS but~~ did not address four or more of the six topics required by Requirement R1. (~~Requirement R1~~ Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (~~Requirement R1~~ Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior	its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~Requirement R 1~~ Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (~~Requirement R1~~ Part 1.2)	containing low impact BCS as required by Requirement R1. (~~Requirement R1~~ Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (~~Requirement R1~~ Part 1.2)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (~~Requirement R1~~ Part 1.2)	the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (~~Requirement R1~~ Part 1.2)		
R2	~~Operations Planning~~	~~Lower~~	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BCS and SCI but~~ failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BCS and SCI but~~ failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2)	The Responsible Entity ~~documented the physical access controls for its assets containing low impact BCS and SCI but~~ failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for~~	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BCS and SCI according to Requirement R2, Attachment 1. (Requirement R2)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity ~~implemented electronic access controls but~~ failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BCS and SCI but~~ failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1,	OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BCS and SCI but~~ failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BCS and SCI but~~ failed to document electronic access controls according to Requirement R2,	~~electronic access controls for its assets containing low impact BCS and SCI but~~ failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BCS and SCI but~~ failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2,	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Section 4. (Requirement R2) OR The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BCS and SCI but~~ failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for TCA~~	Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls but~~ failed to implement authentication for all Dial-up Connectivity that provides access to low impact BCS, per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity ~~documented one or more incident response plan(s) within its cyber~~	Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but~~ failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for TCA and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for TCA	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~and Removable Media, but~~ failed to manage its TCA according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for TCA, but~~ failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	~~security plan(s) for its assets containing low impact BCS and SCI, but~~ failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BCS and SCI but~~ failed to document the determination of whether an identified Cyber Security Incident is a	managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for TCA and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for TCA and Removable Media, but~~ failed to	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for TCA and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1,	implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for TCA and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for TCA managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for TCA and Removable Media, but~~ failed to implement the		

R #	~~**Time Horizon**~~	~~**VRF**~~	**Violation Severity Levels (CIP-003-Y)**			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	~~**Operations Planning**~~	~~**Medium**~~	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	~~**Operations Planning**~~	~~**Lower**~~	The Responsible Entity ~~has identified a delegate by name,~~	The Responsible Entity ~~has identified a delegate by name,~~	The Responsible Entity ~~has identified a delegate by name, title, date of~~	The Responsible Entity ~~has used delegated authority~~

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	~~title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	~~delegation, and specific actions delegated, but~~ did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	~~for actions where allowed by the CIP Standards, but does~~ did not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Modification to CIP Standards Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to

Version	Date	Action	Change Tracking
			identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BCS.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
Y	TBD	Virtualization conforming changes	

Attachment 1

Required Sections for Cyber Security Plan(s) ~~for Assets Containing Low Impact BCS or SCI that supports any part of a Low Impact BCS~~

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, (2) ~~the asset or the locations of the SCI supporting low impact BCS within the asset, and (3)~~ the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BCS ~~and each asset containing SCI that supports any part of a low impact BCS~~ identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- an SCI that supports any part of a low impact BCS,

and a system(s) outside the asset containing:

- ~~the asset containing~~ the low impact BCS; or
- ~~the asset containing~~ the SCI that supports any part of a low impact BCS; and

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or ~~the asset containing the~~ SCI that supports any part of a low impact BCS; and

iii. not used for time-sensitive communication of ~~p~~Protection System. ~~or control functions between intelligent electronic devices.~~

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports any part of a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, or SCI that supports any part of a low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting the TCA to a low impact BCS or the SCI that supports any part of a low impact BCS (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports any part of a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code prior to connecting the Removable Media to a low impact BCS or SCI that supports any part of a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) ~~for Assets Containing Low Impact BCS or SCI that supports any part of a low impact BCS~~

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS or ~~the SCI that supports any part of a low impact BCS~~ within the asset; and
  b. The Cyber ~~Asset(s), VCA, or SCI~~ System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets ~~containing low impact BCS, or SCI that supports any part of a low impact BCS,~~the routable protocol communication as outlined in Section 3 ~~between a low impact BCS, or SCI that supports any part of a low impact BCS, and systems outside the asset~~ is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communication is used for time-sensitive ~~protection or control functions between intelligent electronic devices~~communications between Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) ~~between the low impact BCS, or SCI that supports any part of a low impact BCS, and systems outside the asset containing low impact BCS, or SCI that supports any part of a~~

~~low impact BCS,~~ or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS ~~or SCI that supports any part of a low impact BCS~~).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, controls to maintain the known good state of the OS and software, application whitelisting practices, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update

process, the use of application whitelisting, use of controls to maintain the known good state of the OS and software, or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-Y~~8~~

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-Y~~8~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links, between discrete Electronic Security Perimeters (ESP~~s~~).

~~**4.2.3.2.**~~**4.2.3.3.** Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

~~See Implementation Plan for CIP-003-8.~~

~~3. **Background:**~~

~~Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.~~

~~The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.~~

~~The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.~~

~~Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~N.~~B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact ~~BES Cyber Systems~~BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of ~~BES Cyber Systems~~BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for ~~BES Cyber Systems~~BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS shall implement one or more documented cyber security plan(s) for its low impact ~~BES Cyber Systems~~BCS, and Shared Cyber Infrastructure (SCI) that supports any part of a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact ~~BES Cyber Systems~~BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

~~O.~~C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions. ~~As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.~~

~~1.3.~~**1.2. Evidence Retention:**

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

~~1.4.~~**1.3. Compliance Monitoring and Enforcement Program~~Assessment Processes~~:**

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Investigations~~
- ~~Self-Reporting~~

- ~~Complaints~~

~~1.5. Additional Compliance Information:~~

~~None.~~

Violation Severity Levels

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	~~Operations Planning~~	~~Medium~~	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address one of the nine topics required by Requirement R1. (~~R~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address two of the nine topics required by Requirement R1. (~~R~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address three of the nine topics required by Requirement R1. (~~R~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 17 calendar months but did complete this review in	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address four or more of the nine topics required by Requirement R1. (Part ~~R~~1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1. (~~R~~Part 1.1)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (~~R~~Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16	within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R~~Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17	less than or equal to 18 calendar months of the previous review. (~~R~~Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 by the CIP Senior

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous approval. (~~R~~Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address one of the six topics required by Requirement R1. (~~R~~Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing	calendar months of the previous approval. (~~R~~Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address two of the six topics required by R1. (~~R~~Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES	policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address three of the six topics required by Requirement R1. (~~R~~Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (~~R~~Part 1.2) OR	Manager within 18 calendar months of the previous approval. (~~R~~Part 1.1) OR The Responsible Entity ~~documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but~~ did not address four or more of the six topics required by Requirement R1. (~~R~~Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (~~R~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior	Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 16	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (~~R~~Part 1.2)	impact ~~BES Cyber Systems~~BCS as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (~~R~~Part 1.2)	calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (~~R~~Part 1.2)		
R2	~~Operations Planning~~	~~Lower~~	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~implemented electronic access~~	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR	The Responsible Entity ~~documented the physical access controls for its assets containing low impact BES Cyber Systems, but~~ failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls for its assets~~	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact ~~BES Cyber Systems~~BCS according to Requirement R2, Attachment 1. (Requirement R2)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~controls but~~ failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document electronic access controls according to Requirement R2,	~~containing low impact BES Cyber Systems, but~~ failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented ~~one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2)	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media,~~ but failed to manage its Transient Cyber	Attachment 1, Section 3. (R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls but~~ failed to implement authentication for all Dial-up Connectivity that provides access to low impact ~~BES Cyber System~~BCS(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity ~~documented one or more incident response plan(s) within its cyber security plan(s) for~~	OR The Responsible Entity ~~documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but~~ failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for ~~Transient Cyber Assets~~TCA managed by	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets, but~~ failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	~~its assets containing low impact BES Cyber Systems, but~~ failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document the determination of whether an identified Cyber Security Incident is a	the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber~~	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for ~~Transient Cyber Assets~~TCA managed by the Responsible Entity according to	~~Assets and Removable Media, but~~ failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~BCS according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR		

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	~~Operations Planning~~	~~Medium~~	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has~~ did not identify~~ied~~, by name, a CIP Senior Manager. OR The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				the change. (Requirement R3)		Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	~~Operations Planning~~	~~Lower~~	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has used delegated authority for actions where allowed by the CIP Standards, but~~ does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 60

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar days of the change. (Requirement R4)

~~P.~~D. Regional Variances

None.

~~Q.~~E. Interpretations

None.

~~R.~~F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	

Version	Date	Action	Change Tracking
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Attachment 1

Required Sections for Cyber Security Plan(s) ~~for Assets Containing Low Impact BES Cyber Systems~~

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact ~~BES Cyber Systems~~BCS ratings can utilize policies, procedures, and processes for their high or medium impact ~~BES Cyber Systems~~BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. ~~b~~Between:

- a low impact ~~BES Cyber System(s)~~BCS; or
- An SCI that supports any part of a low BCS ~~and a Cyber Asset(s)~~

and a Cyber System(s) outside the asset containing:

- the low impact ~~BES Cyber System~~BCS(s); or
- the SCI that supports any part of low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact ~~BES Cyber System(s)~~BCS or SCI that supports any part of a low impact BCS; and

iii. not used for time-sensitive ~~protection or control functions between intelligent electronic devices (e.g., ~~communications of Protection Systems~~using protocol IEC TR-61850-90-5 R-GOOSE)~~.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact ~~BES Cyber System(s)~~BCS or SCI that supports any part of a low impact BCS, per ~~Cyber Asset~~system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. ~~Transient Cyber Asset~~TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact ~~BES Cyber Systems~~BCS, through the use of ~~Transient Cyber Assets~~TCA or Removable Media. The plan(s) shall include:

5.1 For T~~ransient Cyber Asset(s)~~TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA~~Transient Cyber Asset~~ capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting ~~the Transient Cyber Asset to a low impact BES Cyber System~~ (per ~~Transient Cyber Asset~~TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code~~use of live operating system and software executable only from read-only media~~;
- Review of system hardening used by the party; or
- Review of ~~O~~other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset~~TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a ~~BES Cyber System~~BCS or SCI that supports any part of a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~BCS or SCI that supports any part of a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) ~~for Assets Containing Low Impact BES Cyber Systems~~

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset; and
  b. The Cyber ~~Asset(s)~~System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by ~~containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound~~ electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications between Protection Systems. ~~is used for time-sensitive protection or control functions between intelligent electronic devices.~~ Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) ~~between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s)~~ or lists of implemented

electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the ~~BES Cyber System~~BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. ~~Transient Cyber Asset~~TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, controls to maintain the known good state of the OS and software, application whitelisting practices,~~ processes to restrict communication,~~ or other method(s) to mitigate the introduction of malicious code. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update

process, the use of application whitelisting, ~~use of live operating systems~~use of controls to maintain the known good state of the OS and software, or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.~~

~~If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.~~

~~Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.~~

~~Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber~~

~~security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.~~

~~For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:~~

~~1.1.1 Personnel and training (CIP-004)~~

~~Organization position on acceptable background investigations~~

~~Identification of possible disciplinary action for violating this policy~~

~~Account management~~

~~Electronic Security Perimeters (CIP-005) including Interactive Remote Access~~

~~Organization stance on use of wireless networks~~

~~Identification of acceptable authentication methods~~

~~Identification of trusted and untrusted resources~~

~~Monitoring and logging of ingress and egress at Electronic Access Points~~

~~Maintaining up-to-date anti-malware software before initiating Interactive Remote Access~~

~~Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access~~

~~Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access~~

~~For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls~~

~~Physical security of BES Cyber Systems (CIP-006)~~

~~Strategy for protecting Cyber Assets from unauthorized physical access~~

~~Acceptable physical access control methods~~

~~Monitoring and logging of physical ingress~~

~~System security management (CIP-007)~~

~~Strategies for system hardening~~

~~Acceptable methods of authentication and access control~~

~~Password policies including length, complexity, enforcement, prevention of brute force attempts~~

~~Monitoring and logging of BES Cyber Systems~~

~~Incident reporting and response planning (CIP-008)~~

~~Recognition of Cyber Security Incidents~~

~~Appropriate notifications upon discovery of an incident~~

~~Obligations to report Cyber Security Incidents~~

~~1.1.6 Recovery plans for BES Cyber Systems (CIP-009)~~

~~Availability of spare components~~

~~Availability of system backups~~

~~1.1.7 Configuration change management and vulnerability assessments (CIP-010)~~

~~Initiation of change requests~~

~~Approval of changes~~

~~Break-fix processes~~

~~1.1.8 Information protection (CIP-011)~~

~~Information access control methods~~

~~Notification of unauthorized information disclosure~~

~~Information access on a need-to-know basis~~

~~1.1.9 Declaring and responding to CIP Exceptional Circumstances~~

~~Processes to invoke special procedures in the event of a CIP Exceptional Circumstance~~

~~Processes to allow for exceptions to policy that do not violate CIP requirements~~

~~For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:~~

~~1.2.1 Cyber security awareness~~

~~Method(s) for delivery of security awareness~~

~~Identification of groups to receive cyber security awareness~~

~~1.2.2 Physical security controls~~

~~Acceptable approach(es) for selection of physical security control(s)~~

~~1.2.3 Electronic access controls~~

~~Acceptable approach(es) for selection of electronic access control(s)~~

~~1.2.4 Cyber Security Incident response~~

~~Recognition of Cyber Security Incidents~~

~~Appropriate notifications upon discovery of an incident~~

~~Obligations to report Cyber Security Incidents~~

~~1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~Acceptable use of Transient Cyber Asset(s) and Removable Media~~

~~Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media~~

~~Method(s) to request Transient Cyber Asset and Removable Media~~

~~1.2.6 Declaring and responding to CIP Exceptional Circumstances~~

~~Process(es) to declare a CIP Exceptional Circumstance~~

~~Process(es) to respond to a declared CIP Exceptional Circumstance~~

~~Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.~~

~~In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.~~

~~Requirement R2:~~

~~The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.~~

~~Requirement R2, Attachment 1~~

~~As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.~~

~~Guidance for each of the subject matter areas of Attachment 1 is provided below.~~

~~Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness~~

~~The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.~~

~~Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.~~

~~Requirement R2, Attachment 1, Section 2 – Physical Security Controls~~

~~The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.~~

~~The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other~~

~~operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.~~

~~The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.~~

~~Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.~~

~~User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.~~

~~Requirement R2, Attachment 1, Section 3 – Electronic Access Controls~~

~~Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.~~

~~When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).~~

~~When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.~~

~~In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the~~

~~exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.~~

~~The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.~~

~~Electronic Access Control Exclusion~~

~~In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.~~

~~Considerations for Determining Routable Protocol Communications~~

~~To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.~~

~~When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.~~

~~Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.~~

~~Determining Electronic Access Controls~~

~~Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.~~

~~Concept Diagrams~~

~~The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.~~

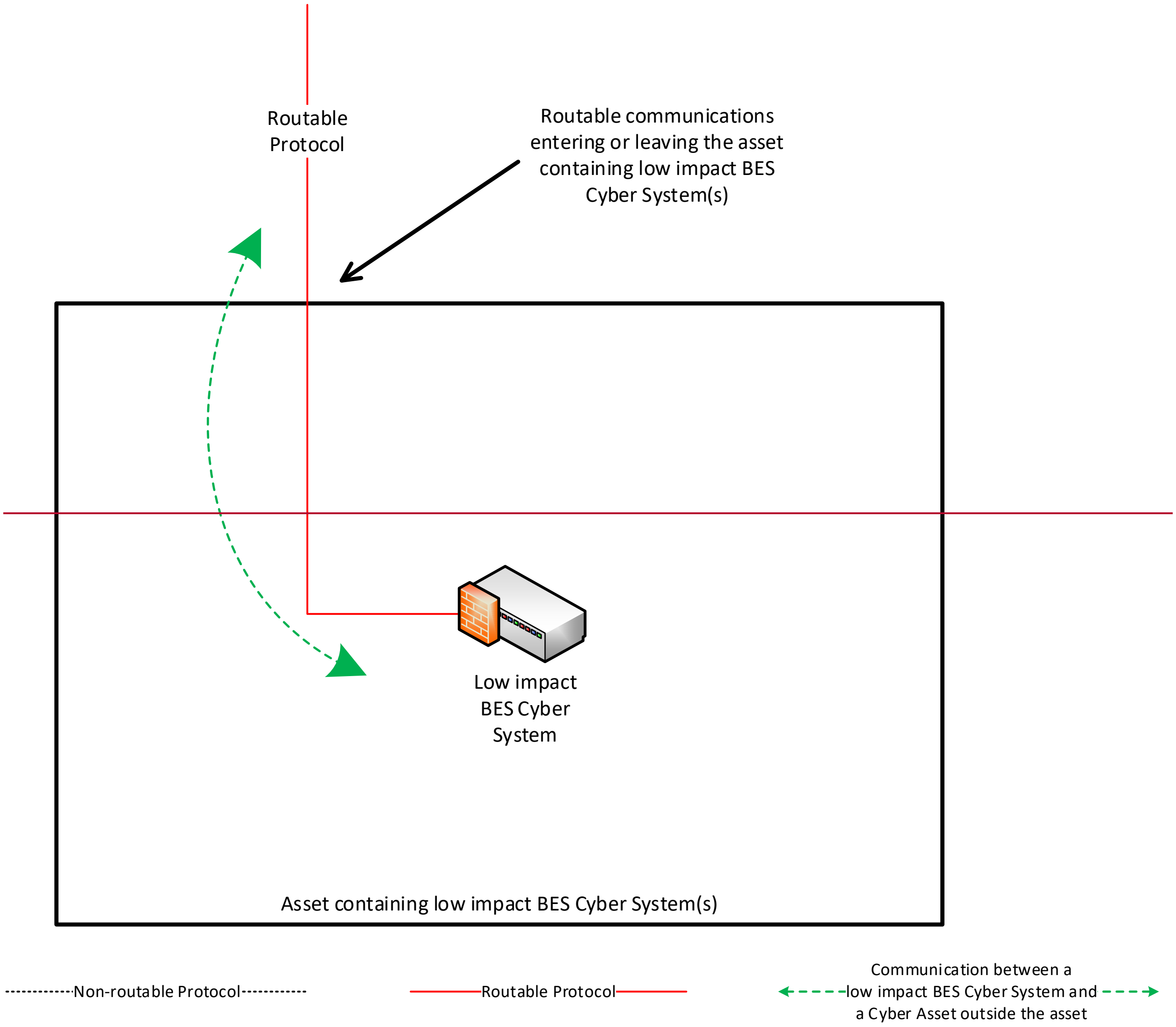
~~NOTE:~~

~~This is not an exhaustive list of applicable concepts.~~

~~The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.~~

~~Reference Model 1 – Host-based Inbound & Outbound Access Permissions~~

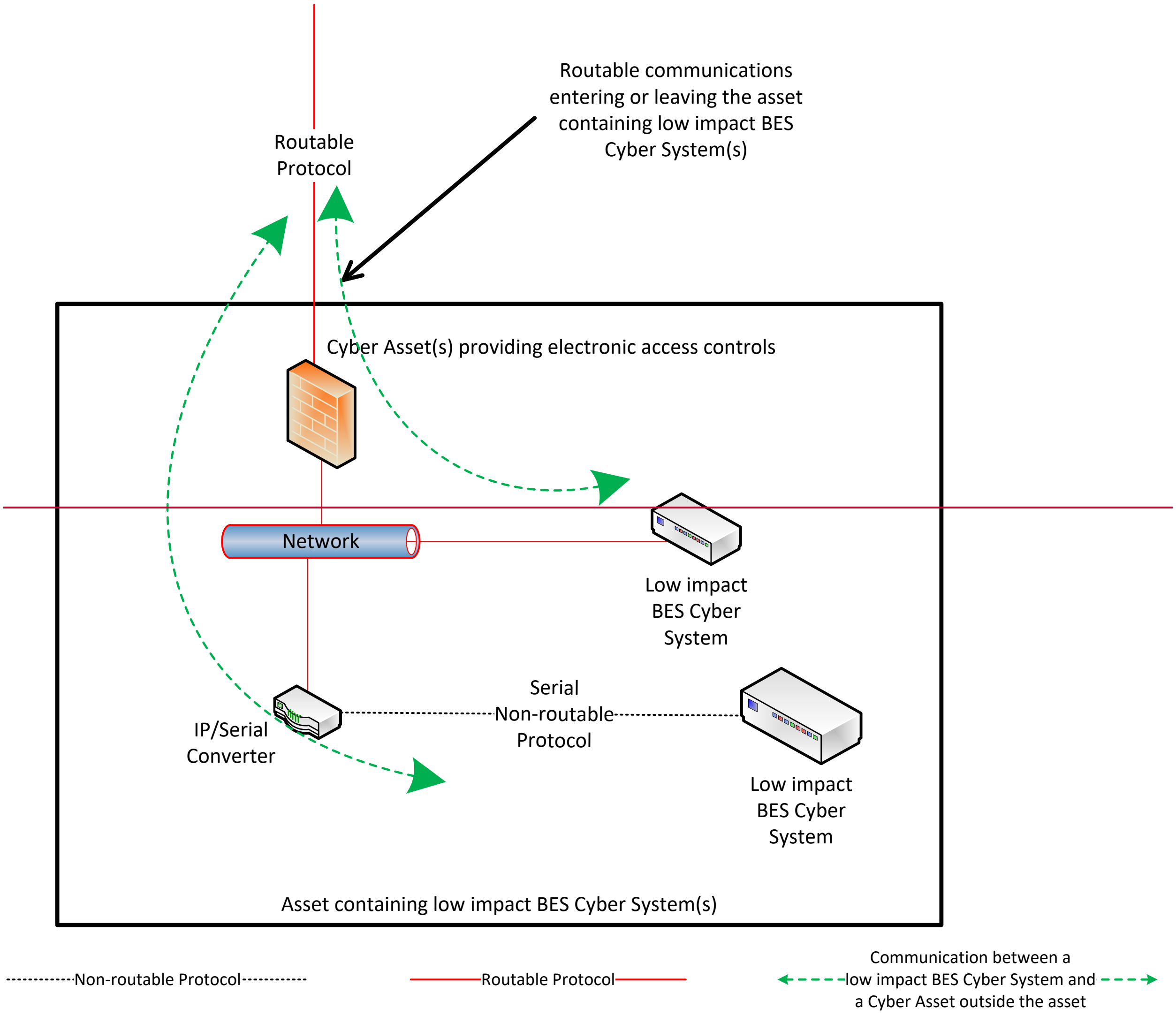
~~The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~Reference Model 1~~

~~Reference Model 2 – Network-based Inbound & Outbound Access Permissions~~

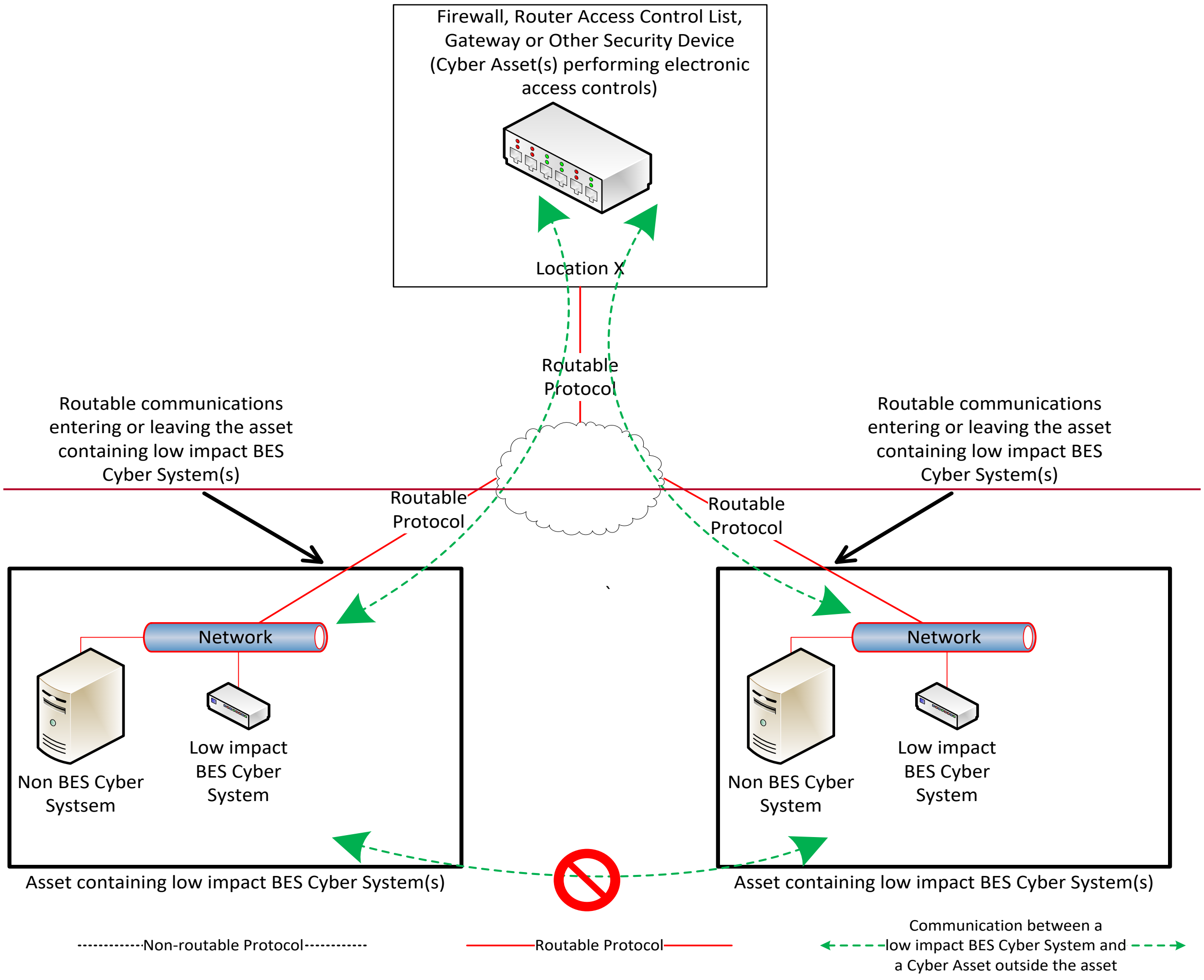
~~The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~Reference Model 2~~

~~Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions~~

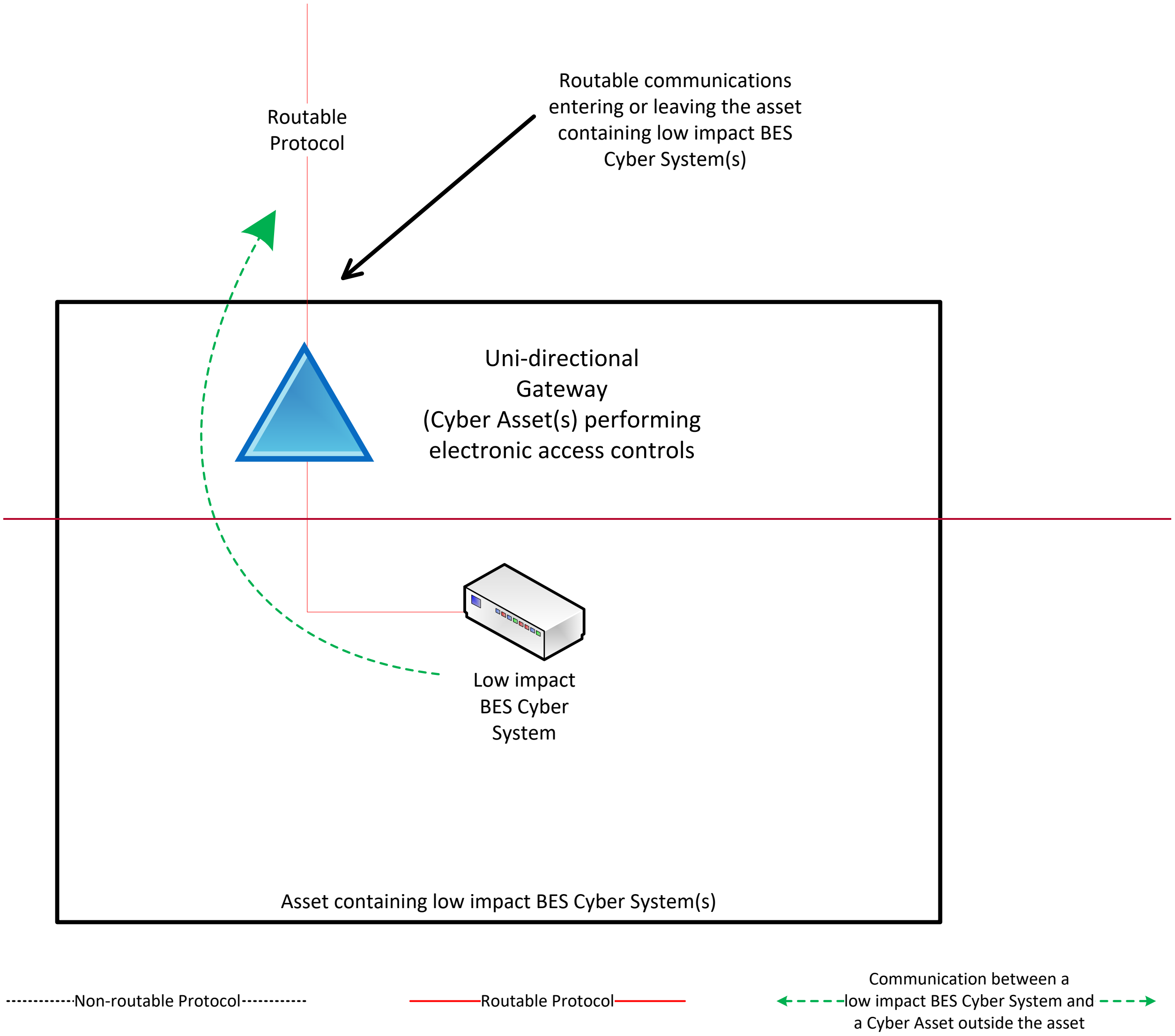
~~The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~



~~Reference Model 3~~

~~Reference Model 4 – Uni-directional Gateway~~

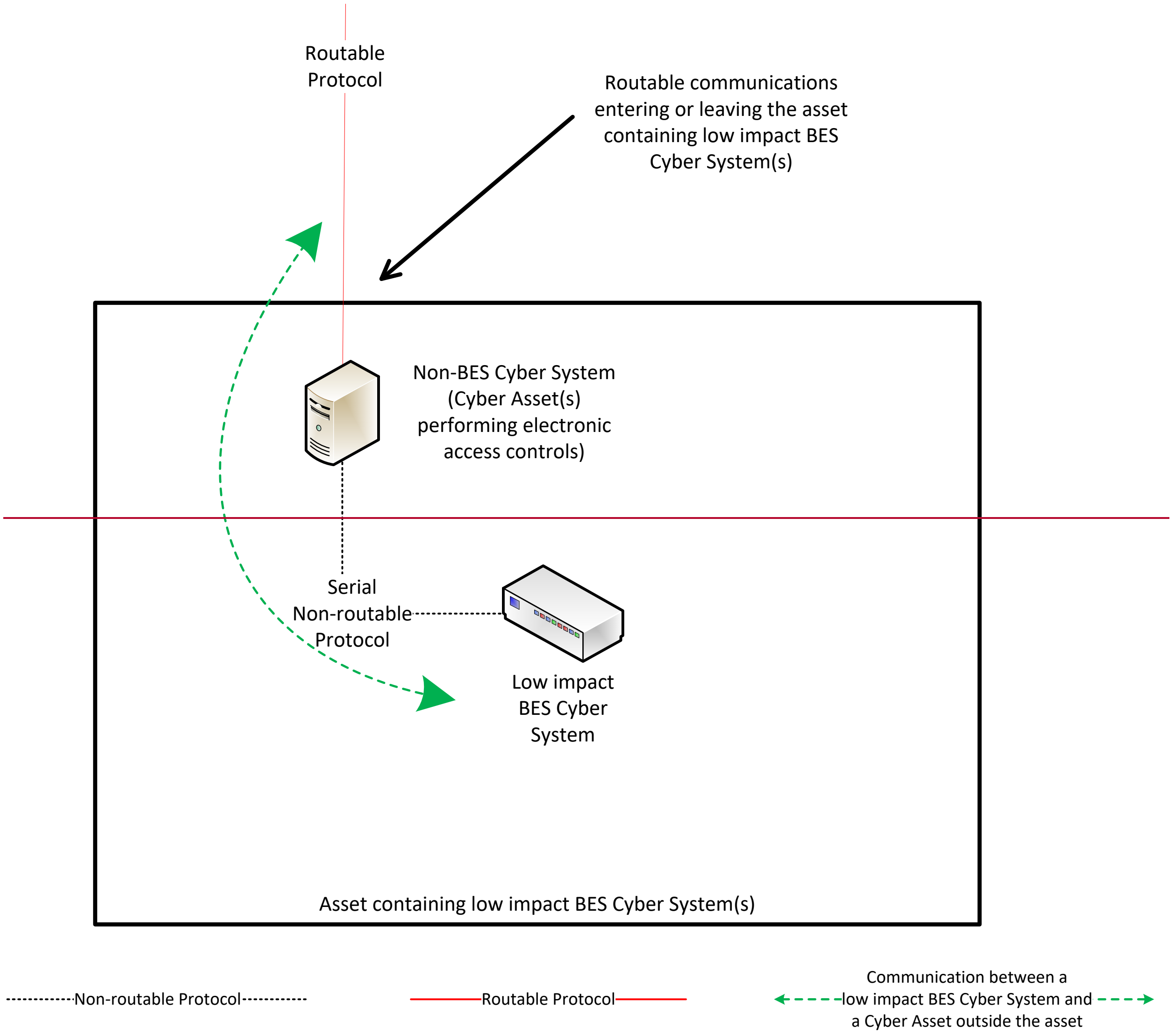
~~The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a “one-way” (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.~~



~~Reference Model 4~~

~~Reference Model 5 – User Authentication~~

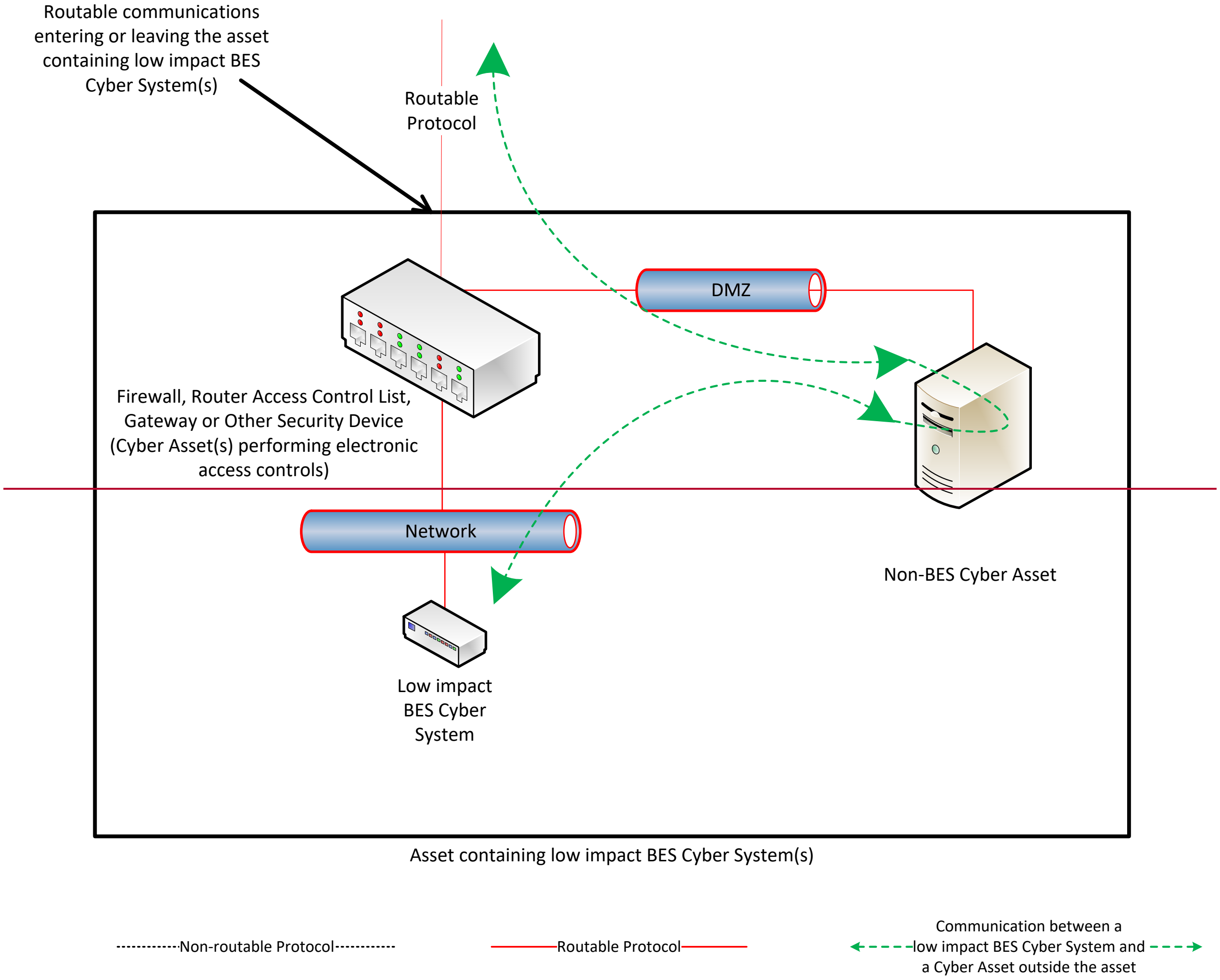
~~This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.~~



~~Reference Model 5~~

~~Reference Model 6 – Indirect Access~~

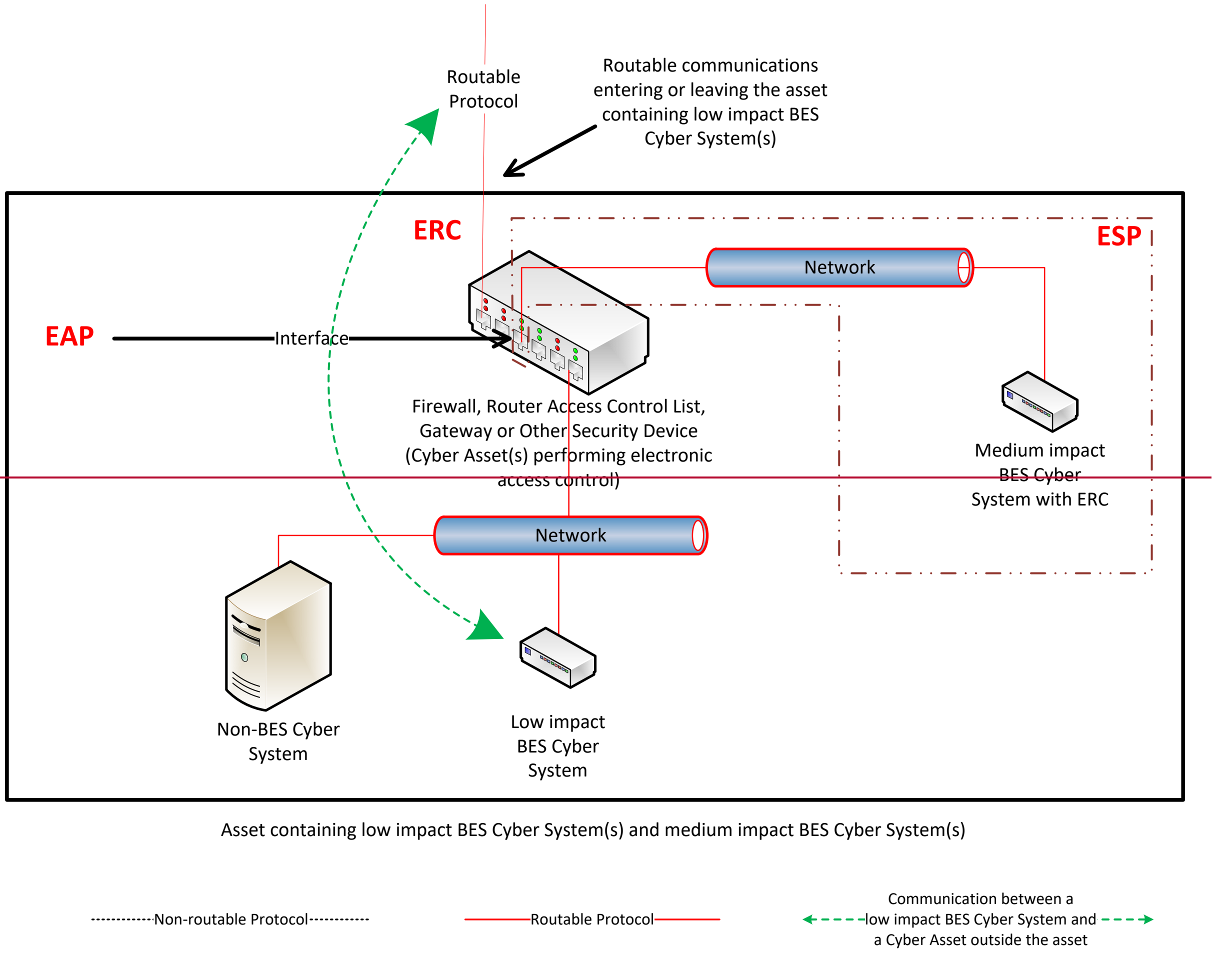
~~In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.~~



~~Reference Model 6~~

~~Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC~~

~~In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.~~



~~Reference Model 7~~

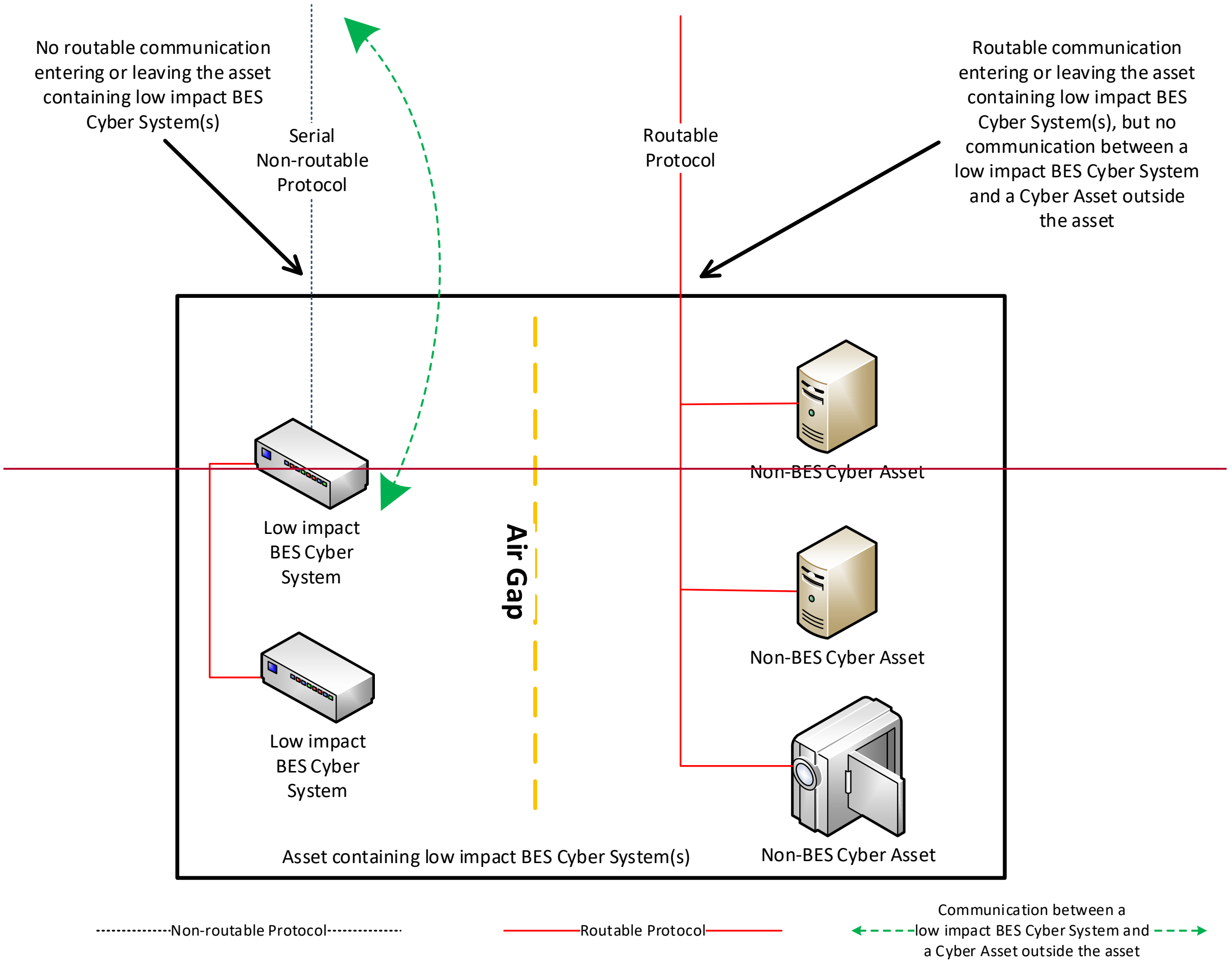
~~Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required~~

~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:~~

~~The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;~~

~~The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.~~

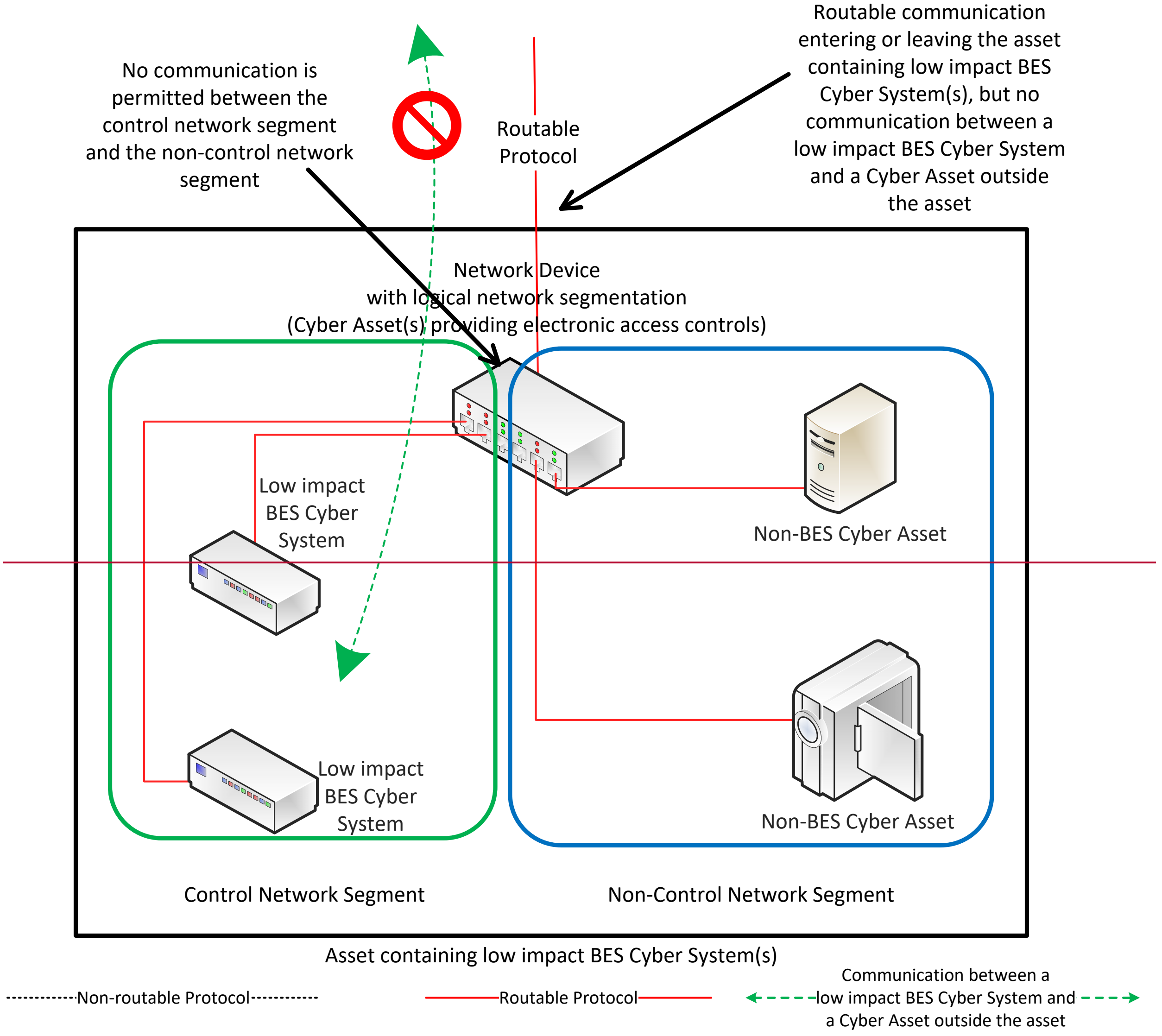
~~The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).~~



~~Reference Model 8~~

~~Reference Model 9 – Logical Isolation - No Electronic Access Controls Required~~

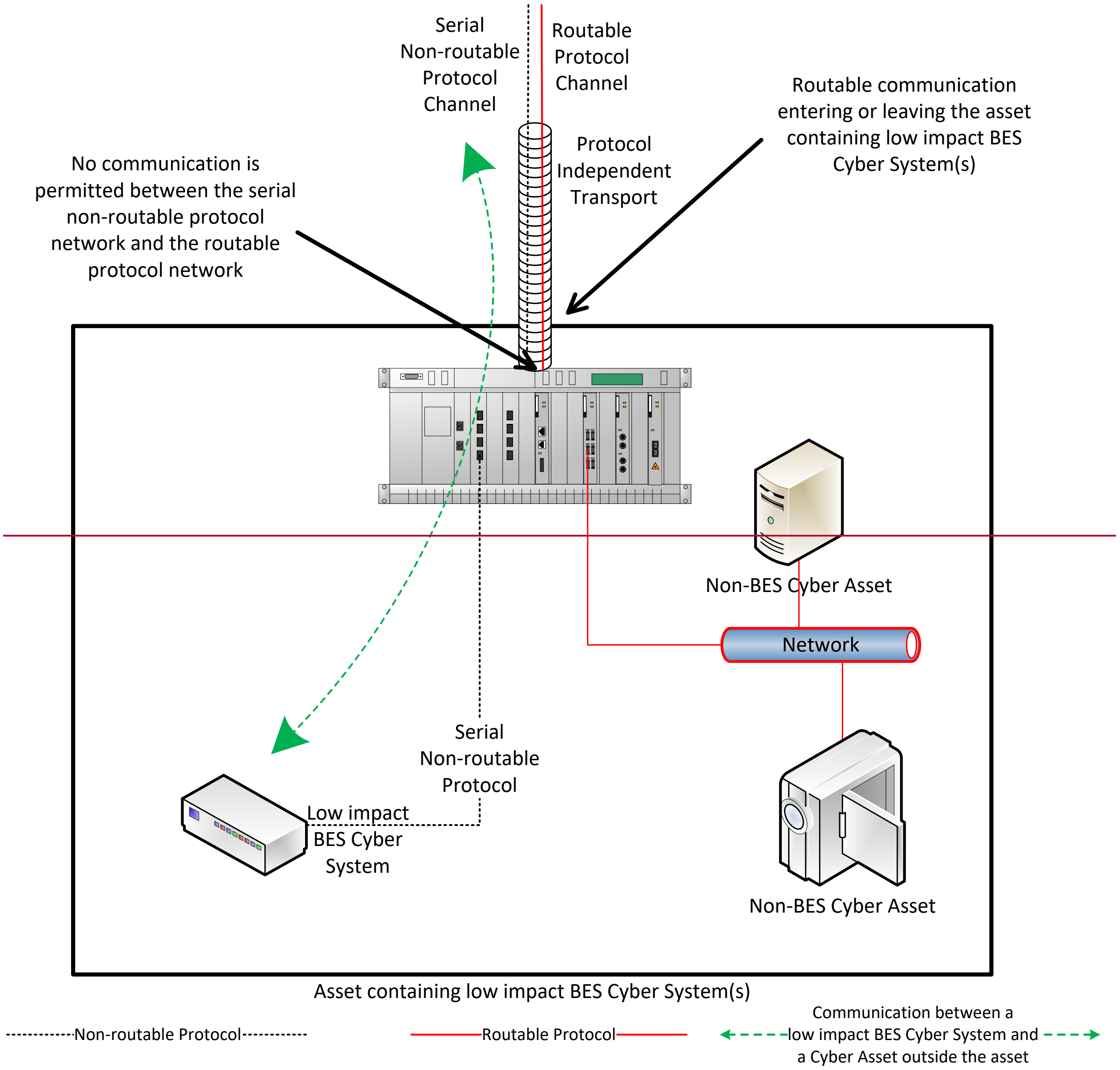
~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.~~



~~Reference Model 9~~

~~Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required~~

~~In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.~~



~~Reference Model 10~~

~~Dial-up Connectivity~~

~~Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.~~

~~Insufficient Access Controls~~

~~Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:~~

~~An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.~~

~~A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.~~

~~Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.~~

~~Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response~~

~~The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.~~

~~Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.~~

~~The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity’s response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.~~

~~For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, “A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.” The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.~~

~~Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.~~

~~Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~Examples of these temporarily connected devices include, but are not limited to:~~

~~Diagnostic test equipment;~~

~~Equipment used for BES Cyber System maintenance; or~~

~~Equipment used for BES Cyber System configuration.~~

~~To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.~~

~~With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.~~

~~Malicious Code Risk Mitigation~~

~~The terms "mitigate", "mitigating", and "mitigation" are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.~~

~~Per Transient Cyber Asset Capability~~

~~As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.~~

~~Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity~~

~~For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.~~

~~**Section 5.1:** Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.~~

~~The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.~~

~~Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~The following is additional discussion of the methods to mitigate the introduction of malicious code.~~

~~Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.~~

~~Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.~~

~~When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.~~

~~If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity~~

~~Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch~~

~~[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014~~

~~management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.~~

~~**Section 5.2.1:** Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.~~

~~Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.~~

~~Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.~~

~~Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.~~

~~Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.~~

~~Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.~~

~~**Section 5.2.2:** The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.~~

~~Requirement R2, Attachment 1, Section 5.3 - Removable Media~~

~~Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.~~

~~**Section 5.3:** Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable~~

~~Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.~~

~~As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.~~

~~Requirement R3:~~

~~The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.~~

~~Requirement R4:~~

~~As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.~~

~~The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.~~

~~Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.~~

~~Rationale for Requirement R2:~~

~~In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.~~

~~Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.~~

~~Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):~~

~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."~~

~~The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".~~

~~The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.~~

~~Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.~~

~~Rationale for Section 5 of Attachment 1 (Requirement R2):~~

~~Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "...provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~Rationale for Requirement R3:~~

~~The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.~~

~~FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given~~

~~the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.~~

~~Rationale for Requirement R4:~~

~~The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

~~In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 3 Definitions"

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-8
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or
   instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.
4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. **Balancing Authority**

   4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. **Generator Operator**

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems”: Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Part	If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Examples of evidence may include, but are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High impact BCS and their associated EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part	Examples of evidence may include, but are not limited to, workflow or sign-off form showing access removal for any individual

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part	5.1) within 30 calendar days of the effective date of the termination action.	BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Version History

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train four or more individuals (with the exception of CIP Exceptional

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	The Responsible Entity did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3)

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	for one individual. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	3.2.2 for two individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	OR The Responsible Entity did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active	The Responsible Entity did not authorize electronic access or	The Responsible Entity did not authorize electronic	The Responsible Entity did not implement any documented

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	unescorted physical access based on need for one individual. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	access or unescorted physical access based on need for two individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	program(s) for access management. (Requirement R4) OR The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R5	The Responsible Entity did not revoke individual's user accounts upon termination action within 30 calendar days of the date of termination action for one or more individuals. (Part 5.3) OR The Responsible Entity did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action for one individual. (Part 5.1) OR The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action for two individuals. (Part 5.1) OR The Responsible Entity for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action for three or more individuals. (Part 5.1) OR The Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity, for one individual, did not authorize provisioned electronic access to	The Responsible Entity, for two individuals, did not authorize provisioned electronic access	The Responsible Entity, for three individuals, did not authorize provisioned	The Responsible Entity did not implement one or more documented

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-004-8)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1)
OR
The Responsible Entity did not perform the verification required by Part 6.2 within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2)
OR
The Responsible Entity, for one individual, did not remove the individual’s ability to use provisioned access to BCSI by the timeframe required in Part 6.3.</td><td>to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1)
OR
The Responsible Entity did not perform the verification required by Part 6.2 within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2)
OR
The Responsible Entity, for two individuals, did remove each individual’s ability to use provisioned access to BCSI by the timeframe required in Part 6.3.</td><td>electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1)
OR
The Responsible Entity did not perform the verification required by Part 6.2 within 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2)
OR
The Responsible Entity, for three individuals, did not remove each individual’s ability to use provisioned access to BCSI by the timeframe required in Part 6.3.</td><td>access management program(s) for BCSI. (Requirement R6)
OR
The Responsible Entity, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1)
OR
The Responsible Entity did not perform the verification required by Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2)
OR
The Responsible Entity, for four or more individuals, did not remove each individual’s ability to use provisioned access to BCSI by the timeframe required in Part 6.3.</td></tr>
</table>

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21– March 22, 2021
~~45~~63-day formal comment period with ballot	June 30 – ~~August 13~~September 1, 2021
45- day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~August 29– October 11, 2021~~
Final Ballot	~~October 19–28, 2021~~April 2022
Board adoption	~~November 4, 2021~~ May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-8~~Y~~

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. Generator Operator

    4.1.4. Generator Owner

    4.1.5. Reliability Coordinator

    4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-8~~Y~~:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002-5.1a identification and categorization processes.

4.3. "Applicable Systems"~~ Columns in Tables~~: Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan"

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8~~Y~~ Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8~~Y~~ Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8~~Y~~ Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact BCS Medium ~~I~~impact BCS Shared Cyber Infrastructure (SCI) ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8~~Y~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8~~Y~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8~~Y~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~I~~impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-8~~Y~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
		Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	
2.2	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8~~Y~~ Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8~~Y~~ Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8~~Y~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

CIP-004-8~~Y~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.2	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI~~ identified independently~~ supporting an Applicable System ~~above~~in this Part	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8~~X~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.3	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-8~~X~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.5	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System above	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 ~~to~~ through 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8~~Y~~ Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8~~Y~~ Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8~~Y~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System ~~above~~in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP).	~~An e~~Example of evidence may include, but ~~is~~ are not limited to, dated documentation of the process to authorize electronic access and unescorted physical access in a ~~Physical Security Perimeter~~PSP.

CIP-004-Y Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

CIP-004-Y Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.3	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~ in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	~~An e~~Examples of evidence may include, but ~~is~~are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8~~Y~~ Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8~~Y~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8~~Y~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.1	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~ in this Part	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

CIP-004-8~~Y~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.2	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~ in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-8~~Y~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High ~~I~~impact BCS and their associated ~~:~~ EACMS SCI ~~identified independently~~ supporting an Applicable System~~ above~~ in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	~~An e~~Examples of evidence may include, but ~~is~~are not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

CIP-004-8~~Y~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.4	High ~~I~~impact BCS and their associated ~~:~~ EACMS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the ~~“~~Applicable Systems~~”~~ identified in *CIP-004-8~~Y~~ Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8~~Y~~ Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8~~Y~~ Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8~~Y~~ Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI~~ identified independently~~ supporting an Applicable System ~~above~~in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8~~Y~~ Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.2	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~ in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program:
As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-8~~Y~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train one individual (with the exception of	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train two individuals (with the exception of CIP	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train three individuals (with the exception of CIP Exceptional	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR

R #	Violation Severity Levels (CIP-004-8~~Y~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~ personnel	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the personnel risk	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing ~~P~~personnel ~~R~~risk ~~A~~assessments~~ (PRAs)~~, for individuals, including contractors and service

R #	Violation Severity Levels (CIP-004-8~~Y~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	conduct the personnel risk assessments~~PRA~~ as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity ~~did conduct Ppersonnel Rrisk Aassessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for one individual. (Part 3.1 & Part 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including~~	risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity ~~did conduct Ppersonnel Rrisk Aassessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for two individuals. (Part 3.1 & Part 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted~~	assessments~~PRA~~ as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity ~~did conduct Ppersonnel Rrisk Aassessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for three individuals. (Part 3.1 & Part 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted~~	vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the personnel risk assessments~~PRA~~ as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for four or more individuals. (Part 3.1 & Part 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal~~

R #	Violation Severity Levels (CIP-004-8~~Y~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 and 3.2.2 for one individual. (Part 3.2 & Part 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate criminal history records check for access authorization for one individual. (Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct	~~physical access but~~ did not include the required checks described in 3.2.1 and 3.2.2 for two individuals. (Part 3.2 & Part 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate criminal history records check for access authorization for two individuals. (Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~ for two individuals with authorized electronic or authorized unescorted physical access within ~~7~~	~~physical access but~~ did not include the required checks described in 3.2.1 and 3.2.2 for three individuals. (Part 3.2 & Part 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate criminal history records check for access authorization for three individuals. (Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~ for three individuals with authorized electronic or authorized unescorted physical access within ~~7~~ seven calendar years of the	~~history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals. (Part 3.2 & Part 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate criminal history records check for access authorization for four or more individuals. (Part 3.3 & Part 3.4) OR The Responsible Entity did not conduct ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~ for four or more individuals with authorized electronic or authorized unescorted physical access within ~~7~~ seven calendar years of the previous personnel risk assessments~~PRA~~ completion date. (Part 3.5)

R #	Violation Severity Levels (CIP-004-8~~Y~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~ for one individual with authorized electronic or authorized unescorted physical access within ~~7~~ seven calendar years of the previous personnel risk assessments~~PRA~~ completion date. (Part 3.5)	seven calendar years of the previous personnel risk assessments ~~PRA~~ completion date. (Part 3.5)	previous personnel risk assessments~~PRA~~ completion date. (Part 3.5)	
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity ~~has implemented~~	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR ~~The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1)~~ The Responsible Entity did not authorize electronic access or unescorted physical access based on

R #	Violation Severity Levels (CIP-004-8~~Y~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	subsequent calendar quarter. ~~-~~(Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	subsequent calendar quarter. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~ did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)
R5	The Responsible Entity ~~has implemented one or more process(es) to~~did not revoke ~~the~~ individual's user	The Responsible Entity ~~has implemented one or more process(es) to~~did not initiate removal~~e~~ of the ability for unescorted	The Responsible Entity ~~has implemented one or more process(es) to~~ did not initiate removal~~e~~ of the ability for unescorted	The Responsible Entity ~~has~~ did not implement~~ed~~ any documented program(s) for access revocation for electronic access or unescorted physical access. (Requirement R5)

R #	Violation Severity Levels (CIP-004-8~~Y~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	accounts upon termination action~~ but did not do so for~~ within 30 calendar days of the date of termination action for one or more individuals. (Part 5.3) OR The Responsible Entity ~~has implemented one or more process(es) to~~ did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer~~, but did not do so for~~ within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity ~~has implemented one or more process(es) to determine and~~	physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual. (Part 5.1) OR The Responsible Entity~~ has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but~~, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for two individuals. (Part 5.1) OR The Responsible Entity~~ has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but~~, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	OR The Responsible Entity~~ has implemented one or more process(es) to~~ did not initiate removal~~e~~ of the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action~~ but did not initiate those removals~~ for three or more individuals. (Part 5.1) OR The Responsible Entity~~ has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but~~, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)

R #	Violation Severity Levels (CIP-004-8~~Y~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~document extenuating operating circumstances following a termination action, reassignment, or transfer, but~~ did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)			
R6	The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform~~ed~~ the	The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. -(Part 6.1) OR The Responsible Entity did not perform~~ed~~ the verification required by ~~Requirement R6~~ Part 6.2	The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. -(Part 6.1) OR The Responsible Entity did not perform~~ed~~ the verification required by ~~Requirement R6~~ Part 6.2	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (Requirement R6) OR The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	verification required by ~~Requirement R6~~ Part 6.2 ~~more than~~within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for one individual, did not remove the individual's ability to use provisioned access to BCSI ~~do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	~~more than~~within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. ~~-~~(Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for two individuals, did not remove each individual's ability to use provisioned access to BCSI ~~do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	~~more than~~ within 17 calendar months but did in less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for three individuals, did not ~~do so~~ remove each individual's ability to use provisioned access to BCSI by the timeframe required in ~~Requirement R6,~~ Part 6.3.	The Responsible Entity did not perform~~ed~~ the verification required by ~~Requirement R6~~ Part 6.2 ~~more than~~wit~~i~~hin 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for four or more individuals, did not remove ~~the~~each individual's ability to use provisioned access to BCSI ~~do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	

Version	Date	Action	Change Tracking
7	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-8~~7~~

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting ~~BES Cyber Systems~~BCS.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-8~~7~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2.~~4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002~~-~~7~~5.1a~~ identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan” ~~for CIP-004-7~~.

~~**Background:** Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *“Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].”* The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple~~

~~high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~
~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8~~7~~ Table R1 – Security Awareness Program

Part	Applicable Systems	Requirements	Measures
1.1	High ~~I~~impact ~~BES Cyber Systems~~BCS Medium ~~I~~impact ~~BES Cyber Systems~~BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to ~~BES Cyber~~Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8~~7~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8~~7~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8~~7~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~I~~impact ~~BES Cyber Systems~~BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for ~~BES Cyber Systems~~BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a ~~BES Cyber System's~~BCS electronic interconnectivity and	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~8~~7 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
		interoperability with other Cyber ~~Assets~~System, including Transient Cyber Assets (TCA), and with Removable Media.	
2.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to ~~a~~Applicable Systems~~Cyber Assets~~, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

CIP-004-8~~7~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS SCI supporting an Applicable System in this Part		

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to ~~BES Cyber Systems~~ Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8~~7~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8~~7~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
	and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium iImpact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated:	Criteria or process for verifying that personnel risk assessments performed	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation

CIP-004-8~~7~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.
3.5	High iImpact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 ~~to~~ through 3.4 within the last seven years.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8~~7~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP).	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a ~~Physical Security Perimeter~~PSP.
4.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium iImpact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated:	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of

CIP-004-8~~7~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part		personnel who have access (i.e., user account listing), or - Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by

CIP-004-8~~7~~ Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
			people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8~~7~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is

CIP-004-8~~7~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS SCI supporting an Applicable System in this Part		not necessary.
5.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the

CIP-004-8~~7~~ Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
		circumstances.	operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the ~~"~~Applicable Systems~~"~~ identified in *CIP-004-8~~7~~ Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8~~7~~ Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8~~7~~ Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1~~.~~) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8~~7~~ Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: - List of authorized individuals; - List of individuals who have been provisioned access; - Verification that provisioned access is appropriate based on need; and - Documented reconciliation actions, if any.
6.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security~~	The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR	The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include four or more of the

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~training program but failed to~~did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. ~~–~~(Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity ~~has a program for conducting~~	The Responsible Entity ~~has a program for conducting~~	The Responsible Entity ~~has a program for conducting~~	The Responsible Entity did not have all of the required elements

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~ personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year~~	~~Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the personnel risk assessments~~PRA~~ as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR	~~Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the personnel risk assessments~~PRA~~ as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR	as described by 3.1 through 3.4 included within documented program(s) for implementing ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the personnel risk assessments~~PRA~~ as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including~~

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	~~criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~ through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR	The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~ through 3.2.2 for two individuals. (Parts 3.2 & 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4)	The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~ through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate criminal history records check for access authorization for three	~~contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~ through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate

R #	**Violation Severity Levels (CIP-004-8~~7~~)**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	The Responsible Entity did not conduct ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~ for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments~~PRA~~ completion date. (Part 3.5)	OR The Responsible Entity did not conduct ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~ for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments~~PRA~~ completion date. (Part 3.5)	individuals. (Parts 3.3 ~~&~~through 3.4) OR The Responsible Entity did not conduct ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~ for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments~~PRA~~ completion date. (Part 3.5)	criminal history records check for access authorization for four or more individuals. (Parts 3.3 ~~&~~through 3.4) OR The Responsible Entity did not conduct ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~ for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments~~PRA~~ completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR ~~The Responsible Entity did not implement one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1)~~

R #	**Violation Severity Levels (CIP-004-8~~7~~)**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	The Responsible Entity ~~has implemented processes to~~ did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for 5% or less of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. ~~-~~(Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 5% but less than (or equal to) 10% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. ~~-~~(Part 4.3)	records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 10% but less than (or equal to) 15% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 15% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity ~~has implemented one or more process(es) to~~did not revoke ~~the~~ individual's user accounts upon termination action ~~but did not do so for~~ within 30 calendar days of the date of termination action for one or more individuals. (Part 5.3) OR The Responsible Entity ~~has implemented one or more process(es) to~~ did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer~~, but did not do so for~~ within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity ~~has implemented one or more~~	The Responsible Entity ~~has implemented one or more process(es) to~~did not initiate removal~~e~~ of the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for one individual. (Part 5.1) OR The Responsible Entity ~~has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~ for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day	The Responsible Entity ~~has implemented one or more process(es) to~~did not initiate removal~~e~~ of the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for two individuals. (Part 5.1) OR The Responsible Entity ~~has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~ for two individuals, did not revoke the authorized electronic access to individual	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity ~~has implemented one or more process(es) to~~did not initiate removal~~e~~ of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for three or more individuals. (Part 5.1) OR The Responsible Entity ~~has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~ for three or more individuals, did not revoke the authorized electronic

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but~~ did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	following the predetermined date. (Part 5.2)	accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. ~~-~~(Part 6.1) OR The Responsible Entity did not perform~~ed~~ the verification required by ~~Requirement R6~~	The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform~~ed~~ the verification required by	The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform~~ed~~ the verification required by	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (Requirement R6) OR The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	Part 6.2 ~~more than~~within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for one individual, did not remove the individual's ability to use provisioned access to BCSI ~~do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	~~Requirement R6~~ Part 6.2 ~~more than~~within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for two individuals, did remove ~~the~~each individual's ability to use provisioned access to BCSI ~~not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	~~Requirement R6~~ Part 6.2 within ~~more than~~ 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for three individuals, did not remove each individual's ability to use provisioned access to BCSI~~do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform~~ed~~ the verification required by ~~Requirement R6~~ Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for four or more individuals, did not ~~do~~ remove ~~the~~each individual's ability to use provisioned access to BCSI ~~so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 3 Definitions"

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-8
3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the BES.
4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1. **Balancing Authority**

      4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

            4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

      4.1.3. **Generator Operator**

      4.1.4. **Generator Owner**

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems”: Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See “Project 2016-02Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCSand their associated PCA Medium impact BCSand their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP.	Examples of evidence may include, but is not limited to, • a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, and deny all other routable protocol communications, through the ESP, excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Physical isolation of an ESP; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that enforce an ESP for an Applicable System in Part 1.1	Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.	Examples of evidence may include, but are not limited to, documentation of the access enforcement configuration or settings to or from the Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the management plane resources (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated PCA Medium impact BCS at Control Centers and their associated PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls (such as encryption), or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time sensitive communication of Protection Systems.	Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).
1.5	High impact BCS with Dial-up Connectivity and their associated PCA Medium impact BCS with Dial-up Connectivity and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Permit authorized Interactive Remote Access (IRA), if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	Intermediate Systems used to access Applicable Systems of Part 2.1	For all IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Examples of evidence may include, but are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls initiate and terminate.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	Intermediate System used to access Applicable Systems of Part 2.1	For all IRA, require multi-factor authentication to the Intermediate System.	Example of evidence may include, but are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High impact BCS with vendor remote access and their associated PCA Medium impact BCS with vendor remote access and their associated PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including IRA and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High impact BCS with vendor remote access and their associated PCA Medium impact BCS with vendor remote access and their associatedPCA SCI supporting an Applicable System in this Part	Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access • (including IRA and system-to-system remote access).
2.6	Intermediate System used to access Applicable Systems of Part 2.1	Routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High impact BCS EACMS and PACS associated with Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High impact BCS EACMS and PACS associated with Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account;

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
			disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the ESP required by Part 1.6.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not protect the Applicable Systems connected to the network with routable protocol with an ESP. (Part 1.1) OR The Responsible Entity did not permit only needed communications to and from Applicable Systems either individually or as a group and deny all other communications. (Part 1.2) OR The Responsible Entity did not permit only needed and controlled communications to and from Management Interfaces for Applicable Systems and deny all other communications. (Part 1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to span a single ESP between PSPs, as required by Part 1.3. OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the Applicable Systems. (Part 1.5)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access	The Responsible Entity did not implement processes for three of the applicable Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote

R #	**Violation Severity Levels**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			(including IRA and system-to-system remote access) (Part 2.5).	access (including IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not ensure routable protocol communications are through an ESP as required by Part 2.6.
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI*. (Requirement R3)	The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for EACMS or SCI supporting EACMS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS or SCI supporting EACMS (Part 3.2). OR	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI*. (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for SCI supporting PACS and EACMS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI supporting PACS and EACMS (Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~second~~ third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
~~45~~63-day formal comment period with ballot	June 30 – ~~August 13~~September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~August 29–October 11, 2021~~
Final Ballot	~~October 19–28, 2021~~April 2022
Board adoption	~~November 4, 2021~~May 2022

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-8

3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperations or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links~~,~~ between the Cyber Systems providing confidentiality and integrity of an ~~Electronic Security Perimeter (~~ESP~~)~~ that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems" ~~Columns in Tables~~: Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See "Project 2016-02 Modification to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter(s)*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter(s)* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP	Examples of evidence may include, but is not limited to, • a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2~~1~~	High ~~I~~impact BCS with ERC and their associated ~~Protected Cyber Asset (~~PCA~~)~~ Medium ~~I~~impact BCS with ERC and their associated PCA	~~Applicable Systems connected to a network via a routable protocol must be protected by an ESP that p~~Permit~~s~~ only needed routable protocol communications and deny~~ies~~ all other communications, through and ESP, excluding time-sensitive communications of ~~p~~Protection Systems~~or control functions between intelligent electronic devices~~. ~~Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.~~	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system~~s~~ and documented reason such as: • Electronic Access Point (EAP) configuration~~ or policies~~; • Physical isolation of an ESP; • Network infrastructure configuration ~~or policies~~ (e.g. technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or ~~policies~~ settings (e.g. technical policies, hypervisor, fabric, back-plane, or SAN configuration); ~~that enforces an ESP and documents the business need.~~

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3~~2~~	SCI ~~identified independently~~ supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that enforce~~s~~ an ESP for ~~the~~ an Applicable System~~s~~ in Part 1.1.	Permit only needed routable protocol~~and controlled~~ communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.	Examples of evidence may include, but are not limited to, documentation of the access enforcemen~~that includes~~ the configuration or settings to or from the Management Interfaces including documented reason~~of systems that enforce access control and ESP~~ such as: • Logical ~~network infrastructure~~ configuration or settings (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multicontext, or multi-tenant environment), • Physically isolated out-of-band network for dedicated Management Interfaces, or • SCI configuration or ~~policies~~ settings showing the isolation of the management plane resources (e.g., technical policies, hypervisor, fabric, back-plane,or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	Applicable Systems	Requirements	Measures
~~1.3~~	~~SCI supporting an Applicable System from Part 1.1.~~	~~Deny network communications from Applicable Systems of Part 1.1 to the Management Interface, per system capability.~~	~~Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems that enforce access control such as:~~ - ~~SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration);~~ - ~~Logical network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multicontext, or multi-tenant environment);~~ - ~~Physically isolated out-of-band network for dedicated~~ - ~~Management Interfaces.~~

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High ~~I~~impact BCS and their associated PCA Medium ~~I~~impact BCS at Control Centers and their associated PCA	Protect the data traversing communication links used to span a single ESP between ~~Physical Security Perimeters (~~PSPs~~)~~ through the use of: • C~~c~~onfidentiality and integrity controls (such as encryption), or • P~~p~~hysical controls that restrict access to the cabling and other nonprogrammable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. ~~t~~Time ~~-~~sensitive protection ~~or control functions between intelligent electronic devices~~communication of Protection Systems.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or ~~policies~~ settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High ~~I~~impact BCS with Dial-up Connectivity and their associated~~:~~ ~~1.~~ PCA; ~~2. PACS hosted on SCI; and~~ ~~3. EACMS hosted on SCI~~ Medium ~~I~~impact BCS with Dial-up Connectivity and their associated~~:~~ ~~1.~~ PCA; ~~2. PACS hosted on SCI; and~~ ~~3. EACMS hosted on SCI~~ SCI supporting an Applicable System ~~above~~in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, per system capability.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to configuration, settings, or~~, a~~ documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection
1.6	High impact BCS ~~EACMS that enforces an ESP for the~~ ~~Applicable Systems in Part 1.1.~~ Medium impact BCS at Control Centers	Have one or more methods for ~~D~~detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. ~~For all IRA and vendor remote access, excluding Dial-up Connectivity, the~~ Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable ~~r~~Requirement ~~p~~Parts in *CIP-005-8 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BCS and their associated~~:~~ PCA Medium ~~I~~impact BCS ~~with ERC~~ and their associated~~:~~ PCA ~~EACMS that enforces an ESP for the Applicable Systems in Part 1.1.~~ SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part ~~Intermediate Systems used to access Applicable Systems of Part 2.1~~	Permit authorized IRA, if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, ~~or Management Systems reports~~ configuration or settings that show all IRA is through an Intermediate System.

CIP-005-8 Table R2 – Remote Access Management			
Part	Applicable Systems	Requirements	Measures
2.2	Intermediate Systems used to access Applicable Systems of Part 2.1	Protect the confidentiality and integrity (e.g., encryption) of IRA between the client and the Intermediate System.	~~An e~~Examples of evidence may include, but ~~is~~are not limited to, architecture documents, ~~or~~ configuration or settings detailing where confidentiality and integrity controls initiate and terminate.
2.3	Intermediate Systems used to access Applicable Systems of Part 2.1	Require multi-factor authentication to the Intermediate System.	~~An e~~Example of evidence may include, but ~~is~~are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High ~~I~~impact BCS with vendor remote access and their associated~~:~~ ~~•~~PCA Medium ~~I~~impact BCS with vendor remote access and their associated~~:~~ ~~•~~ PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Have one or more methods for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including IRA and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High ~~I~~impact BCS with vendor remote access and their associated~~:~~ PCA Medium ~~I~~impact BCS with vendor remote access and their associated~~:~~ PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including IRA and system-to-system remote access.
2.6	Intermediate System~~s~~ used to access Applicable Systems of Part 2.1	~~Implement for~~ Routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP. ~~as follows:~~ ~~**2.6.1.** Restrict VCAs of Intermediate Systems to only share CPU and memory with other Intermediate Systems and their associated SCI.~~ ~~**2.6.2.**~~ ~~Permit only needed and controlled communications between Intermediate Systems and Applicable Systems of Part 2.1.~~	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or ~~Configuration showing that the CPU and memory can only be shared with other IS.~~ • Configuration or settings ~~showing how communications are controlled between the~~of each ~~IS~~ Intermediate System ~~and aApplicable sSystems~~.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS and PACS*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable ~~r~~Requirement ~~p~~Parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, ~~and~~ PACS, and SCI

Part	Applicable Systems	Requirements	Measures
3.1	EACMS and PACS associated with High Impact BCS EACMS and PACS associated with Medium Impact BCS with ERC SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High Impact BCS EACMS and PACS associated with Medium Impact BCS with ERC SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, ~~and~~ PACS, and SCI			
Part	Applicable Systems	Requirements	Measures
			a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority:** "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the ESP required by Part 1.~~1~~6~~ or Part 1.2.2~~.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R1 – ESP*. (Requirement R1) OR The Responsible Entity did not protect the Applicable Systems connected to the network with routable protocol with an ESP. (Part 1.1) OR The Responsible Entity did not permit only needed ~~and controlled~~ communications to and from ~~a~~Applicable ~~s~~Systems either individually or as a group and~~ ESP~~deny all other communications. (Part 1.2~~1~~) OR The Responsible Entity did not permit only needed routable protocol

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				communications to and from Management Interfaces for Applicable Systems and deny all other routable protocol communications. (Part 1.3) ~~The Responsible Entity did not implement, for applicable systems, a method for restricting Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability (Requirement R1 Part 1.2.1)~~ ~~OR~~ ~~The Responsible Entity did not implement, for applicable systems, a method for permitting only needed and controlled communications to and from Management Interfaces and Management~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~Systems, ESP all other communications. (Requirement R1 Part 1.2.2)~~ ~~OR~~ ~~The Responsible Entity did not implement, for applicable systems, a method for denying communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability (Require~~ment R1 Part 1.2.3) OR The Responsible Entity did not implement a method to protect the data traversing communication links, ~~where the~~used to span an single ESP ~~spans multiple~~between ~~Physical Security Perimeters~~PSPs, through the use of confidentiality and integrity controls ~~(such as encryption);~~ or physical controls that restrict access

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				to the cabling and other nonprogrammable communication components (~~Requirement R1~~ Part 1.3) OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the ~~a~~Applicable ~~s~~Systems. (~~Requirement R1~~ Part 1.5~~4~~)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (~~Requirement R2~~ Part 2.4);	The Responsible Entity did not implement processes for three of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			or one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (~~Requirement R2~~ Part 2.5).	remote access) (~~Requirement R2~~ Part 2.4) and one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (~~Requirement R2~~ Part 2.5). ~~OR~~ ~~The Responsible Entity did not implement a method for applicable systems restricting Intermediate Systems to only share CPU and memory with its associated SCI and other Intermediate Systems, per system capability (Requirement R2 Part 2.6.1)~~ OR The Responsible Entity did not ~~implement a method for applicable systems permit only needed and controlled~~require routable protocol communications between each Intermediate

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				Systems and A~~a~~pplicable A~~s~~ystems of Part 2.1 to go through an ESP. (~~Requirement R2~~ Part 2.6~~.2~~).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, ~~and~~ PACS, and SCI*. (Requirement R3)	The Responsible Entity ~~had method(s) as required by Part 3.1 for EACMS, SCI, and Management Modules of SCI but~~ did not have a method to determine authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (~~Requirement R3~~ Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for EACMS, SCI and Management Modules of SCI but~~ did not have a method to terminate authenticated vendor-initiated remote connections for PACS or SCI	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity ~~had method(s) as required by Part 3.1 for PACS, SCI and Management Modules of SCI but~~ did not have a method to determine authenticated vendor-initiated remote connections for EACMS or SCI supporting EACMS (~~Requirement R3~~ Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for PACS, SCI and Management Modules of~~	The Responsible Entity did not implement any processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS ~~and~~ PACS, and SCI*. (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		supporting PACS (~~Requirement R3~~ Part 3.2).	~~SCI but~~ did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS or SCI supporting EACMS (~~Requirement R3~~ Part 3.2). OR The Responsible Entity ~~had method(s) as required by Part 3.1 for PACS and EACMS but~~ did not have a method to determine authenticated vendor-initiated remote connections for SCI supporting PACS ~~or~~ and EACMS~~Management Modules of SCI~~ (~~Requirement R3~~ Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for PACS and EACMS but~~ did not have a	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI supporting PACS ~~or~~and EACMS ~~management Modules of SCI~~ (~~Requirement R3~~ Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- See "Project 2016-02 Virtualization Implementation Plan."
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	
8	TBD	Virtualization modifications and ERC/IRA	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-8~~7~~

3. Purpose: To ~~manage electronic access to~~ protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of ~~by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to~~ misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8~~7~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems”: Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Date:** See ~~Implementation Plan for~~ “Project 2016~~9~~-02~~3~~Modifications to CIP Standards Implementation Plan”.

~~6.~~ ~~**Background:** Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *“Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].”* The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~“Applicable Systems” Columns in Tables:~~

~~Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~
- ~~**High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.~~

- ~~**High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~
- ~~**Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS~~ ~~and their associated ~~:~~ PCA	~~All a~~Applicable Systems ~~Cyber Assets~~ connected to a network via a routable protocol must be protected by an ~~shall reside within a defined~~ ESP.	~~An e~~Examples of evidence may include, but is not limited to, • a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.

CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.2	High ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated ~~:~~ PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated~~:~~ PCA	Permit only needed routable protocol communications, and deny all other routable protocol communications, through the ESP, excluding time sensitive communications of Protection Systems. ~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~	~~An e~~Examples of evidence may include, but ~~is~~are not limited to, documentation that includes the configuration of system and documented reason, such as: ~~network diagrams showing all external routable communication paths and the identified EAPs.~~ • Electronic Access Point (EAP) configuration; • Physical isolation of an ESP; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that enforce an ESP for an Applicable System in Part 1.1 ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability. ~~Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.~~	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation of the access enforcement configuration or settings to or from the Management Interfaces, including documented reasons such as: ~~a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.~~ • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the management plane resources (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).

1.4	High ~~I~~impact ~~BES Cyber Systems~~BCS ~~with Dial-up Connectivity~~ and their associated~~:~~ PCA Medium ~~I~~impact B~~ES Cyber Systems~~CS ~~with Dial-up Connectivity~~at Control Centers and their associated~~:~~ PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls (such as encryption), or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time sensitive communication of Protection Systems. ~~Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.~~	~~An e~~Examples of evidence may include, but ~~is~~are not limited to, ~~documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.~~ documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).
1.5	High impact BCS with Dial-up Connectivity and their associated PCA	Perform authentication when establishing Dial-up Connectivity with	~~An e~~Examples of evidence may include, but are~~is~~ not limited to,

CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
	Medium impact BCS with Dial-up Connectivity and their associated PCA SCI supporting an Applicable System in this Part ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers~~	Applicable Systems, per system capability. ~~Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.~~	configuration, settings, or ~~documentation~~ documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection. ~~that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.~~
1.6	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, ~~where technically feasible~~per system capability, in *CIP-005-8~~7~~ Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8~~7~~ Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS ~~with External Routable Connectivity~~ and their associated ~~:~~ PCA SCI supporting an Applicable System in this Part	Permit authorized Interactive Remote Access (IRA), if any, only through an Intermediate System. ~~For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~	Examples of evidence may include, but are not limited to, network diagrams, ~~or~~ architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	Intermediate Systems used to access Applicable Systems of Part 2.1 ~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~	For all ~~Interactive Remote Access~~ IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System. ~~sessions, utilize encryption that terminates at an Intermediate System.~~	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, architecture documents, configuration or settings detailing where confidentiality and ~~encryption~~integrity controls initiate~~s~~ and terminate~~s~~.

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	• ~~PCA~~		
2.3	Intermediate System used to access Applicable Systems of Part 2.1 ~~High Impact BES Cyber Systems and their associated:~~ • ~~PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ • ~~PCA~~ •	~~Require multi-factor authentication f~~For all ~~Interactive Remote Access~~IRA ~~sessions~~, require multi-factor authentication to the Intermediate System.	~~An e~~Example of evidence may include, but are~~is~~ not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High ~~I~~impact ~~BES Cyber Systems~~BCS with vendor remote access and their associated ~~:~~ ~~•~~ PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with vendor remote access ~~with External Routable Connectivity~~ and their associated ~~:~~ ~~•~~PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including ~~Interactive Remote Access~~ IRA and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High ~~I~~impact ~~BES Cyber Systems~~BCS with vendor remote access and their associated~~:~~ PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~vendor remote access and their associated~~:~~ PCA SCI supporting an Applicable System in this Part	Have one or more method(s) to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access).~~,~~ ~~such as:~~ ~~Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or~~ • ~~Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~
2.6	Intermediate System used to access Applicable Systems of Part 2.1	Routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8~~7~~ Table R3 –Vendor Remote Access Management for EACMS,~~ and~~ PACS, and SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS,~~ and~~ PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High ~~I~~impact ~~BES Cyber Systems~~BCS EACMS and PACS associated with Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC SCI supporting an Applicable System in this Part	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High ~~I~~impact ~~BES Cyber Systems~~BCS EACMS and PACS associated with Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ ERC SCI supporting an Applicable System in this Part	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in

CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS, ~~and~~ PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
			a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious ~~communications for both inbound and outbound~~ Internet Protocol (IP) communications entering or leaving the ESP required by Part 1.6. ~~(1.5)~~	The Responsible Entity did not document one or more processes for *CIP-005-8~~6~~ Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not protect the Applicable Systems connected to the network with routable protocol with an ESP. (Part 1.1) OR ~~The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1)~~ OR The Responsible Entity did not permit only needed communications to and from Applicable Systems either individually or as a

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				group and deny all other communications. (Part 1.2) OR The Responsible Entity did not permit only needed and controlled communications to and from Management Interfaces for Applicable Systems and deny all other communications. (Part 1.3) OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to span a single ESP between PSPs, as required by Part 1.3. OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the Applicable Systems. (Part 1.5) ~~External Routable Connectivity through the~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~ESP was not through an identified EAP. (1.2)~~ ~~OR~~ ~~The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)~~ ~~OR~~ ~~The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)~~
R2.	The Responsible Entity does not have documented processes for one or more of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions	The Responsible Entity did not implement processes for three of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5).	~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not ensure routable protocol communications are through an ESP as required by Part 2.6.
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS,* ~~*and*~~ *PACS, and SCI*. (Requirement R3)	The Responsible Entity ~~had method(s) as required by Part 3.1 for EACMS but~~ did not have a method to determine authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by~~	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity ~~had method(s) as required by Part 3.1 for PACS but~~ did not have a method to determine authenticated vendor-initiated remote	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS,* ~~*and*~~ *PACS, and SCI*. (Requirement R3) OR The Responsible Entity did not have any methods as

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		~~Part 3.2 for EACMS but~~ did not have a method to terminate authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.2).	connections for EACMS or SCI supporting EACMS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for PACS but~~ did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS or SCI supporting EACMS (Part 3.2). OR The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for SCI supporting PACS and EACMS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections or control the	required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			ability to reconnect for SCI supporting PACS and EACMS (Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 20~~19-03~~16-02
- CIP-005-8~~7~~ Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 3 Definitions"

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 **Balancing Authority**

   4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 **Generator Operator**

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems”: Each table has an “Applicable Systems” column to define the scope of systems to which a specific Requirement Part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium impact BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC	Define operational or procedural controls to restrict physical access.	Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.
1.2	Medium impact BCS with ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA)	Utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated: 1. EACMS; and 2. PCA	Utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, per system capability.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.4	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a PSP.	Examples of evidence may include, but are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a PSP.
1.5	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a PSP and additional evidence that the alarm or alert was issued and communicated as identified in the Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC	Monitor each PACS for unauthorized physical access to a PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.
1.7	PACS associated with: • High impact BES Cyber Systems, or • Medium impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.
1.8	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each PSP, with information to identify the individual and date and time of entry.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes logging and recording of physical entry into each PSP and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each PSP that show the individual and the date and time of entry into each PSP.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days.	Examples of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP that show the date and time of entry into each PSP.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.1	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each PSP.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	PACS associated with: • High impact BCS, or • Medium impact BCS with ERC Locally mounted hardware or devices at the PSP associated with: • High impact BCS, or • Medium impact BCS with ERC	Maintenance and testing of each PACS and locally mounted hardware or devices at each PSP at least once every 24 calendar months to ensure they function properly.	Examples of evidence may include, but are not limited to, a maintenance and testing program that provides for testing each PACS and locally mounted hardware or devices associated with each applicable each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. **Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. **Compliance Monitoring and Assessment Processes:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				physical access point into a PSP. (Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each PACS for unauthorized physical access to a PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each PSP with sufficient information to identify the individual and date and time of

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least 90 days. (Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance	The Responsible Entity has documented and implemented a maintenance	The Responsible Entity has documented and implemented a maintenance	The Responsible Entity did not document or implement a maintenance and testing program

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Part 3.1)	and testing program for Physical Access Control Systems and locally mounted hardware or devices at the PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	and testing program for PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Part 3.1)	for PACS and locally mounted hardware or devices at the PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for PACS and locally mounted hardware or devices at the PSP, but did not complete required testing within 27 calendar months. (Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~initial~~third draft of proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
~~45~~63-day formal comment period with ballot	June 30 – ~~August~~September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~August 29–October 11, 2021~~
Final Ballot	~~October 19–28, 2021~~April 2022
Board adoption	~~November 4, 2021~~May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 3 Definitions"

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems~~,~~ associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. "Applicable Systems" ~~Columns in Tables~~: Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan"

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium ~~I~~impact BCS without External Routable Connectivity (ERC) ~~SCI without ERC hosting Medium Impact BCS~~ Physical Access Control Systems (PACS) associated with: • High ~~I~~impact BCS • Medium ~~I~~impact BCS with ERC ~~SCI, identified independently supporting an Applicable System above, not included in the Applicable Systems of Part 1.2 or Part 1.3~~	Define operational or procedural controls to restrict physical access.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation that operational or procedural controls exist.

CIP-006-7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.2	Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PCA ~~SCI, identified independently supporting an Applicable System above, not included in the Applicable Systems of Part 1.3~~	Utilize at least one physical access control to allow unescorted physical access into each applicable ~~Physical Security Perimeter~~PSP to only those individuals who have authorized unescorted physical access.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in the physical security plan that describes each ~~Physical Security Perimeter~~PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA ~~SCI identified independently supporting an Applicable System above~~	Utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access, per system capability.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in the physical security plan that describes ~~the~~ each ~~Physical Security Perimeters~~PSP and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PCA ~~SCI identified independently supporting an Applicable System above~~	Monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP.
1.5	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PCA ~~SCI identified independently supporting an Applicable System above~~	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a ~~Physical Security Perimeter~~PSP and additional evidence that the alarm or alert was issued and communicated as identified in the ~~BES~~ Cyber Security Incident response plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

CIP-006-7 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.6	Physical Access Control Systems (PACS) associated with: - High ~~I~~impact BCS, or Medium ~~I~~impact BCS with ERC ~~SCI identified independently supporting an Applicable System above~~	Monitor each ~~Physical Access Control System~~PACS for unauthorized physical access to a ~~Physical Access Control System~~PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.
1.7	~~Physical Access Control Systems (~~PACS~~)~~ associated with: - High ~~I~~impact BCS, or - Medium ~~I~~impact BCS with ERC ~~SCI identified independently supporting an Applicable System above~~	Issue an alarm or alert in response to detected unauthorized physical access to a ~~Physical Access Control System~~PACS to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to each PACS ~~Physical Access Control Systems~~ and additional evidence that the alarm or alerts was issued and communicated as identified in the ~~BES~~ Cyber Security Incident response plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-7 Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.8	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PCA ~~SCI identified independently supporting an Applicable System above~~	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each ~~Physical Security Perimeter~~PSP, with information to identify the individual and date and time of entry, except during CIP Exceptional Circumstances.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in the physical security plan that describes logging and recording of physical entry into each ~~Physical Security Perimeter~~PSP and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each ~~Physical Security Perimeters~~PSP that show the individual and the date and time of entry into each PSP~~Physical Security Perimeter~~.
1.9	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PCA ~~SCI identified independently supporting an Applicable System above~~	Retain physical access logs of entry of individuals with authorized unescorted physical access into each ~~Physical Security Perimeter~~PSP for at least ~~ninety~~ 90 calendar days, except during CIP Exceptional Circumstances.	~~An e~~Examples of evidence may include, but ~~is~~are not limited to, dated documentation such as logs of physical access into each ~~Physical Security Perimeters~~PSP that show the date and time of entry into ~~Physical Security Perimeter~~PSP.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PCA ~~SCI identified independently supporting an Applicable System above~~	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each ~~Physical Security Perimeter~~PSP.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each ~~Physical Security Perimeters~~PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-7 Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.2.	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact BCS with EERC and their associated: 1. EACMS; and 2. PCA ~~SCI identified independently supporting an Applicable System above~~	Require manual or automated logging of visitor entry into and exit from ~~the Physical Security Perimeter~~each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in a visitor control program that requires continuous escorted access of visitors within P~~hysical Security Perimeters~~each PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; and 2. PCA ~~SCI identified independently supporting an Applicable System above~~	Retain visitor logs for at least ~~ninety~~ 90 calendar days.	~~An e~~Examples of evidence may include, but is not limited to, documentation showing logs have been retained for at least ~~ninety~~ 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented ~~Physical Access Control System~~PACS maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented ~~Physical Access Control System~~PACS maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	~~Physical Access Control Systems (~~PACS~~)~~ associated with: - High ~~I~~impact BCS - Medium ~~I~~impact BCS with ERC - ~~SCI identified independently supporting a High Impact BCS; or~~ - ~~SCI identified independently supporting a Medium Impact BCS with ERC~~ Locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP associated with: - High ~~I~~impact BCS - Medium ~~I~~impact BCS with ERC - ~~SCI identified independently supporting a High Impact BCS; or~~ - ~~SCI identified independently supporting a Medium Impact BCS with ERC~~	Maintenance and testing of each ~~Physical Access Control System~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~each PSP at least once every 24 calendar months to ensure they function properly.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, a maintenance and testing program that provides for testing each ~~Physical Access Control System~~PACS and locally mounted hardware or devices associated with each applicable ~~Physical Security Perimeter~~each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-006-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td>**R1**</td><td>N/A</td><td>N/A</td><td>N/A</td><td>The Responsible Entity did not document or implement physical security plans. (Requirement R1)
OR
The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (~~Requirement R1~~ Part 1.1)
OR
The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (~~Requirement R1~~ Part 1.2)
OR
The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (~~Requirement R1~~ Part 1.3)
OR
The Responsible Entity does not have a process to monitor for unauthorized</td></tr>
</table>

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				access through a physical access point into a ~~Physical Security Perimeter~~PSP. (~~Requirement R1~~ Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP or to communicate such alerts within 15 minutes to identified personnel. (~~Requirement R1~~ Part 1.5) OR The Responsible Entity does not have a process to monitor each ~~Physical Access Control System~~PACS for unauthorized physical access to a ~~Physical Access Control Systems~~PACS. (~~Requirement R1~~ Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to ~~Physical Access Control Systems~~PACS or to communicate such alerts within 15 minutes to identified personnel. (~~Requirement R1~~ Part 1.7)

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (~~Requirement~~ Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (~~Requirement R1~~ Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (~~Requirement R2~~ Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (~~Requirement R2~~ Part 2.2)

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ~~ninety~~90 days. (~~Requirement R2~~ Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (~~Requirement R3~~ Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (~~Requirement R3~~ Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (~~Requirement R3~~ Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP. (Requirement R3 Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required testing within 27 calendar months. (~~Requirement R3~~ Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See "Project 2016-02 Modification to CIP Standards Implementation Plan"

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to

Version	Date	Action	Change Tracking
			use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes and CEC language added	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7~~6~~

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-7~~6~~:

4.2.3.1 Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5.1~~ identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific Requirement Part applies.

5. Effective Dates:

See "Project 2016-02 Modifications to CIP Standards Implementation Plan"~~ for CIP-006-6~~.

~~6. Background:~~

~~Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

~~High Impact BES Cyber Systems~~ ~~– Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~Medium Impact BES Cyber Systems~~ ~~– Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~Medium Impact BES Cyber Systems without External Routable Connectivity~~ ~~– Only applies to medium impact BES Cyber Systems without External Routable Connectivity.~~

~~Medium Impact BES Cyber Systems with External Routable Connectivity~~ ~~– Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~Electronic Access Control or Monitoring Systems (EACMS)~~ ~~– Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber~~

~~System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS) –** Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Protected Cyber Assets (PCA) –** Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7~~6~~ Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7~~6~~ Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.1	Medium ~~I~~impact ~~BES Cyber Systems~~BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High ~~I~~impact BCS~~BES Cyber Systems~~, or • Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC	Define operational or procedural controls to restrict physical access.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation that operational or procedural controls exist.

CIP-006-7~~6~~ Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA)	Utilize at least one physical access control to allow unescorted physical access into each applicable ~~Physical Security Perimeter~~PSP to only those individuals who have authorized unescorted physical access.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, language in the physical security plan that describes each ~~Physical Security Perimeter~~PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA	~~Where technically feasible, u~~Utilize two or more different physical access controls (this does not require two completely independent ~~physical access control systems~~PACS) to collectively allow unescorted physical access into ~~Physical Security Perimeters~~PSP to only those individuals who have authorized unescorted physical access, per system capability.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, language in the physical security plan that describes ~~the~~ each PSP~~Physical Security Perimeters~~ and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7~~6~~ Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP.

CIP-006-7~~6~~ Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.5	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP to the personnel identified in the ~~BES~~ Cyber Security Incident response plan within 15 minutes of detection.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a ~~Physical Security Perimeter~~PSP and additional evidence that the alarm or alert was issued and communicated as identified in the ~~BES~~ Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: - High ~~I~~impact ~~BES Cyber Systems~~BCS, or - Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC	Monitor each ~~Physical Access Control System~~PACS for unauthorized physical access to a ~~Physical Access Control System~~PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	~~Physical Access Control Systems (~~PACS~~)~~ associated with: • High ~~I~~impact BES Cyber Systems, or • Medium ~~I~~impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a ~~Physical Access Control System~~PACS to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to ~~Physical Access Control Systems~~PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the ~~BES~~ Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-7~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.8	High i~~I~~mpact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each ~~Physical Security Perimeter~~PSP, with information to identify the individual and date and time of entry.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in the physical security plan that describes logging and recording of physical entry into each ~~Physical Security Perimeter~~PSP and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into ~~Physical Security Perimeters~~each PSP that show the individual and the date and time of entry into ~~Physical Security Perimeter~~each PSP.

CIP-006-7~~6~~ Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each ~~Physical Security Perimeter~~PSP for at least ~~ninety~~ 90 calendar days.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, dated documentation such as logs of physical access into each ~~Physical Security Perimeters~~PSP that show the date and time of entry into each ~~Physical Security Perimeter~~PSP.

~~CIP-006-6 Table R1 — Physical Security Plan~~

~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~1.10~~	~~High Impact BES Cyber Systems and their associated:~~ ~~PCA~~ ~~Medium Impact BES Cyber Systems at Control Centers and their associated:~~ ~~PCA~~	~~Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.~~ ~~Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:~~ • ~~encryption of data that transits such cabling and components; or~~ • ~~monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or~~ • ~~an equally effective logical protection.~~	~~An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.~~

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7~~6~~ Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each ~~Physical Security Perimeter~~PSP~~, except during CIP Exceptional Circumstances~~.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in a visitor control program that requires continuous escorted access of visitors within each ~~Physical Security Perimeters~~PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-7~~6~~ Table R2 – Visitor Control Program

Part	Applicable Systems	Requirements	Measures
2.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from ~~the Physical Security Perimeter~~each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, language in a visitor control program that requires continuous escorted access of visitors within ~~Physical Security Perimeters~~each PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ~~ninety~~ 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ~~ninety~~ 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7~~6~~ Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	~~Physical Access Control Systems (~~PACS~~)~~ associated with: - High ~~I~~impact ~~BES Cyber Systems~~BCS, or - Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC Locally mounted hardware or devices at the ~~Physical Security Perimeter~~ PSP associated with: - High ~~I~~impact ~~BES Cyber Systems~~BCS, or - Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC	Maintenance and testing of each ~~Physical Access Control System~~PACS and locally mounted hardware or devices at ~~the Physical Security Perimeter~~each PSP at least once every 24 calendar months to ensure they function properly.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, a maintenance and testing program that provides for testing each ~~Physical Access Control System~~PACS and locally mounted hardware or devices associated with each applicable ~~Physical Security Perimeter~~each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

2. Table of Compliance Elements

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP. (Part 1.4)

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~ PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each ~~Physical Access Control System~~PACS for unauthorized physical access to a ~~Physical Access Control Systems~~PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to ~~Physical Access Control Systems~~PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each ~~Physical Security Perimeter~~PSP with sufficient information to identify the individual and date and time of entry. (Part

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9) ~~OR~~ ~~The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)~~
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ~~ninety~~ 90 days. (Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months.	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for ~~Physical Access Control Systems~~ PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required testing within 27 calendar months. (Part 3.1)

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	(Part 3.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of	

Version	Date	Action	Change Tracking
		Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~General:~~

~~While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.~~

~~Requirement R1:~~

~~Methods of physical access control include:~~

- ~~Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~
- ~~Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~
- ~~Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~

- ~~Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.~~

~~Methods to monitor physical access include:~~

- ~~Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.~~
- ~~Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.~~

~~Methods to log physical access include:~~

- ~~Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.~~
- ~~Video Recording: Electronic capture of video images of sufficient quality to determine identity.~~
- ~~Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.~~

~~The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.~~

~~Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.~~

~~The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the~~

~~physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.~~

~~This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.~~

~~The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.~~

~~The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an "an equally effective logical protection" in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.~~

~~The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity's BES Cyber Systems while not requiring controls to be~~

~~implemented on third-party components when entities rely on leased third-party communications.~~

~~In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.~~

~~Requirement R2:~~

~~The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.~~

~~The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.~~

~~Requirement R3:~~

~~This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.~~

~~Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable~~

~~communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.~~

~~Rationale for Requirement R2:~~

~~To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.~~

~~Rationale for Requirement R3:~~

~~To ensure all Physical Access Control Systems and devices continue to function properly.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 3 Definitions".

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See Project 2016-02 Modifications to CIP Standards Implementation Plan for CIP-007-7.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1– System Hardening

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports and network accessible logical services, individually or by group. • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; or • Configuration or settings of host-based firewalls or other device level mechanisms that disables or prevents unneeded network accessible logical ports or network accessible logical services.

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium impact BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Examples of evidence may include, but are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting: High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.	Examples of evidence may include, but are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.
2.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Examples of evidence may include, but are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part		
2.3	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.
2.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Examples of evidence may include, but are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part		

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of evidence may include, but are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
	associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part		these processes when malicious code is detected.
3.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Examples of evidence may include, but are not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BCS is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events (per Cyber Asset or BCS capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
	this Part		
4.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use.
5.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Identify individuals who have authorized access to shared accounts.	Examples of evidence may include, but are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information:

None

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)	The Responsible Entity had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization. (Part 1.3)	The Responsible Entity neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days	The Responsible Entity did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2)	The Responsible Entity did not include any processes for installing cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R2. (Requirement R2) OR The Responsible Entity did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity did not obtain approval by the CIP

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	but less than 50 calendar days of the evaluation completion. (Part 2.3)	OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	security patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)	Senior Manager or delegate. (Part 2.4) OR The Responsible Entity did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)
R3	N/A	The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3). OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity missed one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	The Responsible Entity missed one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity did not retain applicable security	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity, per system capability, did not detect

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity missed two or more 15 calendar day intervals. (Part 4.4)	and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)
R5	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity did not, per device capability, change known default passwords. (Part 5.4) OR

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity process(es) for password-only authentication for interactive user access did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity neither limited the number of unsuccessful authentication attempts nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining

Version	Date	Action	Change Tracking
			directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~second~~ third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
45-day formal comment period with ballot	June 30 – ~~August 13~~September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~August 29–October 11, 2021~~
Final Ballot	~~October 19–28, 2021~~April 2022
Board adoption	~~November 4, 2021~~May 2022

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems” ~~Columns in Tables~~:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~I~~impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above.~~in this Part	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. ~~Enable only network accessible Internet Protocol (IP) ports (or services if unable to determine ports) determined to be needed by the Responsible Entity, including port ranges where needed to handle dynamic ports, per system capability. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.~~	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible ~~IP~~ logical ports and network accessible logical services~~or services, individually or by group~~. • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; or • Configuration or settings of host-based firewalls~~, policy,~~ or other device level mechanisms that disables or prevents unneeded network accessible logical services. ~~only allow needed IP ports or services and deny all others.~~

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~I~~impact BCS and their associated: 1. PCA; and 2. Non-programmable communications components located inside both a PSP and ESP~~.~~ Medium ~~I~~impact BCS at Control Centers and their associated: 1. PCA; and 2. Non-programmable communications components located inside both a PSP and ESP~~.~~ SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI ~~identified independently~~ supporting: • High ~~I~~impact BCS and their associated: 1. EACMS 2. PACS; and 3. PCA • Medium ~~I~~impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization. ~~Prevent the sharing of the CPU and memory of Management Interfaces of SCI with non-CIP Systems.~~	Examples of evidence may include, but ~~is~~are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared~~ with non-CIP Systems~~.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.1	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above.~~in this Part	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable ~~s~~Systems that are updateable and for which a patching source exists.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.3	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: - Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of ~~BES Cyber System C~~component software revision, or registry exports that show software has been installed); or - A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.

CIP-007-7 Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.4	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System in this Part~~above~~	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Protection [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Protection

Part	Applicable Systems	Requirements	Measures
3.1	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Deploy method(s) to deter, detect, or prevent malicious code.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, white-listing, privileged introspection, etc.).

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: - Records of response processes for malicious code detection - Records of the performance of these processes when malicious code is detected.

CIP-007-7 Table R3 – Malicious Code Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an applicable system ~~above~~in this Part	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BCS is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, at a minimum, each of the following types of events~~,~~ (per Cyber Asset or BCS ~~system~~ capability: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, ~~any~~ findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.
5.2	High ~~I~~impact BCS and their associated:	Identify and inventory all known enabled default or other generic account types,	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, a

CIP-007-7 Table R5 – System Access Controls			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	either by system, by groups of systems, by location, or by system type(s).	listing of accounts by account types showing the enabled default or generic account types in use.
5.3	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI- ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Identify individuals who have authorized access to shared accounts.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Change known default passwords, per system capability.	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique.
5.5	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable System; and 5.5.2 Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.6	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account lockout parameters; or Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

	~~above~~in this Part		

C. Compliance

1. **Compliance Monitoring Process:**

    1.1. **Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

    1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

    The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

    - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
    - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
    - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

    1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that include the applicable items in CIP-007-7 Table R1. (Requirement R1)~~N/A~~	The Responsible Entity ~~has implemented and documented processes for system hardening but~~ had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (~~Requirement R1~~ Part 1.2) ~~OR~~ ~~The Responsible Entity has implemented and documented processes for system hardening, but has not prevented the sharing of the CPU and memory of Management Interfaces of SCI with non-CIP Systems. (Requirement R1 Part 1.4)~~	The Responsible Entity ~~has implemented and documented processes for determining necessary system hardening, but~~ had one or more unneeded network accessible services enabled. (Requirement R1 Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization. ~~implemented and documented processes for determining necessary system hardening, but had one or more unneeded services enabled.~~ (Requirement R1 Part 1.3)	The Responsible Entity ~~did not~~neither implemented nor document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)

R #	**Violation Severity Levels (CIP-007-7)**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R2	The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (~~Requirement R2~~ Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for ~~a~~Applicable ~~s~~Systems. (~~Requirement R2~~ Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (~~Requirement R2~~ Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the~~	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for installing cyber security patches for Applicable Systems. (~~Requirement R2~~ Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (~~Requirement R2~~ Part 2.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R2. (Requirement R2) OR The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for tracking, evaluating, or installing cyber security patches for applicable ~~systems~~Cyber Assets. (~~Requirement R2~~ Part 2.1) OR The Responsible Entity ~~documented a mitigation plan for an~~

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Requirement R2 Part 2.3)	~~vulnerabilities exposed by applicable security patches,~~ did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (~~Requirement R2~~ Part 2.3)	The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (~~Requirement R2~~ Part 2.3)	~~applicable cyber security patch and documented a revision or extension to the timeframe but~~ did not obtain approval by the CIP Senior Manager or delegate. (~~Requirement R2~~ Part 2.4) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch but~~ did not implement the plan as created or revised within the timeframe specified in the plan. (~~Requirement R2~~ Part 2.4)
R3	N/A	The Responsible Entity ~~has implemented one or more documented process(es), but~~, where signatures or patterns are	The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention~~	The Responsible Entity did not implement or document one or more process(es) that

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		used, the Responsible Entity did not address testing the signatures or patterns. (~~Requirement R3~~ Part 3.3)	~~but~~ did not mitigate the threat of detected malicious code. (~~Requirement R3~~ Part 3.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity~~ did not update malicious code protections. (~~Requirement R3~~ Part 3.3).	included the applicable items in CIP-007-7 Table R3. (Requirement R3). OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not deploy method(s) to deter, detect, or prevent malicious code. (~~Requirement R3~~ Part 3.1)
R4	The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar~~	The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but~~ missed ~~an~~ one 15 calendar day interval and completed the review within 30	The Responsible Entity ~~has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but~~ did not generate alerts	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R4. (Requirement R4) OR

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	~~days but~~ missed ~~an~~one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (~~Requirement R4~~ Part 4.4)	calendar days of the prior review. (~~Requirement R4~~ Part 4.4)	for all of the required types of events described in 4.2.1 through 4.2.2. (~~Requirement R4~~ Part 4.2) OR The Responsible Entity ~~has documented and implemented one or more process(es) to log applicable events identified in 4.1 (except during CIP Exceptional Circumstances) but~~ did not retain applicable event logs for at least the last 90 consecutive days. (~~Requirement R4~~ Part 4.3) OR The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling~~	The Responsible Entity ~~has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but~~ did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (~~Requirement R4~~ Part 4.1)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~of logged events at least every 15 calendar days but~~ missed two or more 15 calendar day intervals. (~~Requirement R4~~ Part 4.4)	
R5	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (~~Requirement R5~~ Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (~~Requirement R5~~ Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification or inventory of ~~-~~all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (~~Requirement R5~~ Part 5.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification of the individuals with authorized	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R5. (Requirement R5) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (~~Requirement R5~~ Part 5.1)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to shared accounts. (~~Requirement R5~~ Part 5.3) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (~~Requirement R5~~ Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access that~~ did not technically or procedurally enforce one of the two password parameters as described in	OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (~~Requirement R5~~ Part 5.1) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but~~ did not, per device capability, change known default passwords. (~~Requirement R5~~ Part 5.4) OR

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-007-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td>5.5.1 and 5.5.2. (~~Requirement R5~~ Part 5.5)
OR
The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (~~Requirement R5~~ Part 5.6)</td><td>The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity~~ did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (~~Requirement R5~~ Part 5.5)
OR
The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or</td></tr>
</table>

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				an obligation to change the password within 18 calendar months of the last password change. (5.6) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Control but, did not~~ neither limit the number of unsuccessful authentication attempts nor generate alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- See "Project 2016-02 ~~Virtualization~~ Modifications to CIP Standards Implementation Plan".
- See Technical Rationale for CIP-007-7

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to

Version	Date	Action	Change Tracking
			use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	TBD	Virtualization modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7~~6~~

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~4.1.6~~4.1.5 Reliability Coordinator

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-007-7~~6~~:

4.2.3.1 Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-~~5.1~~7 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates:

See Project 2016-02 Modifications to CIP Standards Implementation Plan for CIP-007-7"~~6~~.

~~6. Background:~~

~~Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a~~

~~program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~

~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R1 – ~~Ports and Services~~System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R1 – ~~Ports and Services~~System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. ~~Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.~~	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports and network accessible logical services~~on all applicable Cyber Assets and Electronic Access Points~~, individually or by group. • Listings of the listening ports ~~on the Cyber Assets~~, individually or by group, from either ~~the device~~ configuration files or settings, command output (such as netstat), or network scans of open ports; or • Configuration or settings ~~files~~ of host-based firewalls or other device level mechanisms that disables or prevents unneeded network accessible logical ~~only allow needed~~ ports or network accessible logical services~~and deny all others~~.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting: High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	A patch management process for tracking, evaluating, and installing cyber security patches~~ for applicable Cyber Assets~~. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for ~~applicable Cyber Assets~~Applicable Systems that are updateable and for which a patching source exists.	~~An e~~Examples of evidence may include, but ~~is~~are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored~~, whether on an individual BES Cyber System or Cyber Asset basis~~.

CIP-007-7~~6~~ Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security~~-related~~ patches released by the documented sources at least once every 35 calendar days.

CIP-007-7~~6~~ Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; or - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: - Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of ~~BES Cyber System C~~component software revision, or registry exports that show software has been installed); or - A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.

CIP-007-7~~6~~ Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Deploy method(s) to deter, detect, or prevent malicious code.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-7~~6~~ Table R3 – Malicious Code Prevention

Part	Applicable Systems	Requirements	Measures
3.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Log security events, per system capability, ~~at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)~~ for identification of, ~~and after-the-fact investigations of,~~ Cyber Security Incidents that include~~s~~, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the ~~BES Cyber System~~BCS is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-7~~6~~ Table R4 – Security Event Monitoring

Part	Applicable Systems	Requirements	Measures
4.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Generate alerts for security events that the Responsible Entity determines necessitates an alert~~,~~ that includes, as a minimum, each of the following types of events (per Cyber Asset or ~~BES Cyber System~~BCS capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7~~6~~ Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Where technically feasible, r~~Retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, ~~any~~ findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Have a method(s) to enforce authentication of interactive user access, ~~where technically feasible~~per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7~~6~~ Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use ~~for the BES Cyber System~~.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Identify individuals who have authorized access to shared accounts.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Change known default passwords, per ~~Cyber Asset~~system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the ~~Cyber Asset~~Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the ~~Cyber Asset~~Applicable System.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Where technically feasible, f~~For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Where technically feasible, either:~~ Limit the number of unsuccessful authentication attempts~~;~~ or ~~G~~generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: - Documentation of the account-lockout parameters; or - Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.10.~~1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1) ~~N/A~~	The Responsible Entity ~~has implemented and documented processes for Ports and Services but~~ had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity ~~has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,~~ had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization. (Part 1.3)	The Responsible Entity ~~did not~~ neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity ~~has documented and implemented one or~~	The Responsible Entity ~~has documented or implemented one or more~~	The Responsible Entity ~~has documented or implemented one or more~~	The Responsible Entity did not implement or document one or more process(es) that included the

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan,	~~process(es) for patch management but~~ did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for ~~a~~Applicable Systems ~~Cyber Assets~~. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR	~~process(es) for patch management but~~ did not include any processes for installing cyber security patches for ~~a~~Applicable Systems ~~Cyber Assets~~. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but,~~	applicable items in CIP-007-7~~6~~ Table R2. (Requirement R2) OR The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but~~ did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch but~~ did not implement the plan as

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	~~in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)	created or revised within the timeframe specified in the plan. (Part 2.4)
R3	N/A	The Responsible Entity ~~has implemented one or more documented process(es), but~~, where signatures or patterns are used, the Responsible Entity did not address testing the	The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not mitigate the threat of detected malicious code. (Part 3.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (R3). OR

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		signatures or patterns. (Part 3.3)	The Responsible Entity, ~~has implemented one or more documented process(es) for malicious code prevention, but~~ where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but~~ missed one of 15 calendar day ~~an~~ interval and completed the review within 22	The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15-calendar days but~~ missed ~~an~~ one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity ~~has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but~~ did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity ~~has documented and~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity, per system capability, ~~has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but~~ did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar days of the prior review. (Part 4.4)		~~implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but~~ did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but~~ missed two or more 15 calendar day intervals. (Part 4.4)	

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification or inventory of ~~-~~all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity ~~has implemented one or more documented process(es) for~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~password-only authentication for interactive user access that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented~~ process(es) for password-only authentication for interactive user access ~~that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for~~	The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but~~ did not, per device capability, change known default passwords. (Part 5.4) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity~~ did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	to change the password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either~~neither limited the number of unsuccessful authentication attempts nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.~~

~~**1.1.** This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'~~

~~**1.2.** Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.~~

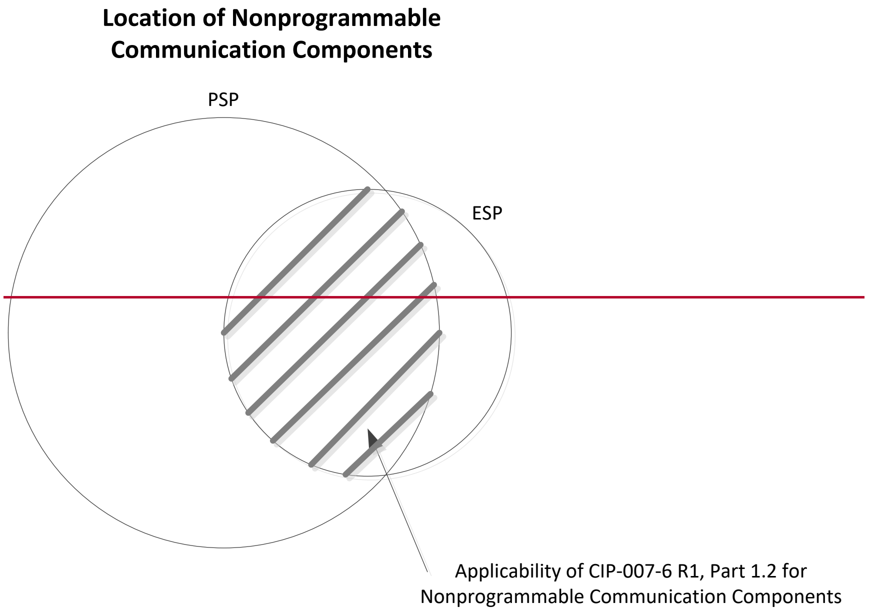
~~The protection of these ports can be accomplished in several ways including, but not limited to:~~

- ~~Disabling all unneeded physical ports within the Cyber Asset's configuration~~
- ~~Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization~~
- ~~Physical port obstruction through removable locks~~

~~The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.~~

~~This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.~~

~~The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:~~



~~**Requirement R2:**~~

~~The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.~~

~~Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.~~

~~One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.~~

~~**2.1.** The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they~~

~~can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.~~

~~**2.2.**~~ ~~Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.~~

~~When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.~~

~~**2.3.**~~ ~~The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or~~

~~those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.~~

~~**2.4.** The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.~~

~~**Requirement R3:**~~

~~**3.1.** Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.~~

~~**3.2.** When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or~~

~~method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.~~

~~Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.~~

~~**3.3.** In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.~~

~~**Requirement R4:**~~

~~Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.~~

~~**4.1.** In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.~~

~~Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.~~

~~User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.~~

~~It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.~~

~~**4.2.** Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.~~

~~The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:~~

- ~~Detected known or potential malware or malicious activity~~
- ~~Failure of security event logging mechanisms~~
- ~~Login failures for critical accounts~~
- ~~Interactive login of system accounts~~
- ~~Enabling of accounts~~
- ~~Newly provisioned accounts~~
- ~~System administration or change tasks by an unauthorized user~~
- ~~Authentication attempts on certain accounts during non-business hours~~
- ~~Unauthorized configuration changes~~
- ~~Insertion of Removable Media in violation of a policy~~

~~**4.3** Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.~~

~~**4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-~~

~~time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.~~

~~**Requirement R5:**~~

~~Account types referenced in this guidance typically include:~~

- ~~Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.~~
- ~~Individual user account: An account used by a single user.~~
- ~~Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.~~
- ~~System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.~~
- ~~Application account: A specific system account, with rights granted at the application level often used for access into a Database.~~
- ~~Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.~~
- ~~Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.~~
- ~~Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.~~

~~**5.1** Reference the Requirement's rationale.~~

~~**5.2** Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.~~

~~**5.3** Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.~~

~~**5.4.** Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.~~

~~The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.~~

~~**5.5.** Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.~~

~~Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.~~

~~**5.6** Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.~~

~~**5.7** Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.~~

~~Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.~~

~~In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.~~

~~The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).~~

~~Rationale for Requirement R2:~~

~~Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.~~

~~Rationale for Requirement R3:~~

~~Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.~~

~~Rationale for Requirement R4:~~

~~Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.~~

~~Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.~~

~~Rationale for Requirement R5:~~

~~To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.~~

~~Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.~~

~~Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.~~

~~Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.~~

~~For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.~~

~~The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.~~

~~The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.~~

~~The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.~~

~~Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning
2. **Number:** CIP-008-7
3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.
4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the Bulk Electric System (BES):

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BES) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated Electronic Access Control and Monitoring Systems (EACMS) Medium impact BCS and their associated EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the Applicable Systems column for this Part; and	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column including justification for attempt determination criteria and documented processes for notification.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
		1.2.3 To provide notification per Requirement R4.	
1.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the Applicable Systems column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	Examples of evidence may include, but are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

M4.

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	Examples of evidence may include, but are not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column according to the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and CISA, or their successors.
4.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and CISA, or their successors.

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
		the Applicable Systems column for this Part.	
4.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and CISA, or their successors.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	N/A	N/A	The Responsible Entity did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible Entity's plan did not include one or more processes to provide notification per Requirement R4. (Part 1.2) OR The Responsible Entity's plan did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	The Responsible Entity did not develop a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible Entity's plan did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the Applicable Systems column for Part 1.2. (Part 1.2)
R2	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 18 calendar months

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months between tests of the plan(s). (Par 2.1)	months between tests of the plan(s). (Part 2.1)	months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column for Part 2.2 occurs. (Part 2.2)	between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the Applicable Systems column for Part 2.3. (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1) OR The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
		calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR The Responsible Entity did not update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	
R4	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not report on one or more of the	The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not notify E-ISAC or CISA, or their	The Responsible Entity did not notify E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3) OR The Responsible Entity did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)	Applicable Systems column. (Requirement R4)	successors, of a Reportable Cyber Security Incident. (Requirement R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
~~45~~63-day formal comment period with ballot	June 30 – ~~August 13~~September 1, 2021
45-day formal comment period with ballot	February 18, 2022

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~August 29– October 11, 2021~~
Final Ballot	~~October 19–28, 2021~~April 2022
Board adoption	~~November 4, 2021~~May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1 Balancing Authority

    4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2 Each Remedial Action Scheme (RAS) where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3 Generator Operator

    4.1.4 Generator Owner

    4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Remedial Action Scheme~~RAS where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems with communication networks and data ~~associated with~~ communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BCS) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”~~ Columns in Tables~~:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*.

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.1	High ~~I~~impact BCS and their associated Electronic Access Control and Monitoring Systems (~~:~~ EACMS) Medium ~~I~~impact BCS and their associated~~:~~ EACMS Shared Cyber Infrastructure (SCI) ~~identified independently~~ supporting an Applicable System above	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~I~~impact BCS and their associated~~:~~ EACMS Medium ~~I~~impact BCS and their associated~~:~~ EACMS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the “Applicable Systems” column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column including justification for attempt determination criteria and documented processes for notification.
1.3	High ~~I~~impact BCS and their associated~~:~~ EACMS Medium ~~I~~impact BCS and their associated~~:~~ EACMS SCI ~~identified independently~~ supporting an Applicable System above	The roles and responsibilities of Cyber Security Incident response groups or individuals.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.4	High ~~I~~impact BCS and their associated ~~:~~ EACMS Medium ~~I~~impactBCS and their associated~~:~~ EACMS SCI ~~identified independently~~ supporting an Applicable System above	Incident handling procedures for Cyber Security Incidents.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BCS and their associated ~~:~~ EACMS Medium ~~I~~impact BCS and their associated~~:~~ EACMS SCI~~ identified independently~~ supporting an Applicable System ~~above~~in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations-based exercises.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.2	High ~~I~~impact BCS and their associated~~:~~ EACMS Medium ~~I~~impact BCS and their associated~~:~~ EACMS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the “Applicable Systems” column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High ~~I~~impact BCS and their associated ~~:~~ EACMS Medium ~~I~~impact BCS and their associated~~:~~ EACMS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the “Applicable Systems” column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~I~~impact BCS and their associated~~:~~ EACMS Medium ~~I~~impact BCS and their associated~~:~~ EACMS SCI~~ identified independently~~ supporting an Applicable System ~~above~~in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.2	High ~~I~~impact BCS and their associated~~:~~ EACMS Medium ~~I~~impact BCS and their associated~~:~~ EACMS SCI ~~identified independently~~ supporting an Applicable System above	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA)~~CISA~~, or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column according to the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~I~~impact BCS and their associated~~:~~ EACMS Medium ~~I~~impact BCS and their associated~~:~~ EACMS SCI~~ identified independently~~ supporting an Applicable System in this Part~~above~~	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and CISA.

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High ~~I~~impact BCS and their associated~~:~~ EACMS Medium ~~I~~impact BCS and their associated~~:~~ EACMS SCI~~ identified independently~~ supporting an Applicable System in this Part~~above~~	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and CISA.
4.3	High ~~I~~impact BCS and their associated~~:~~ EACMS Medium ~~I~~impact BCS and their associated~~:~~ EACMS SCI~~ identified independently~~ supporting an Applicable System in this Part~~above~~	Provide updates, if any, within seven~~7~~ calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and CISA, or their successors.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. Compliance Enforcement Authority: The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

   1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Processes: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Table of Compliance Elements

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (~~Requirement R1~~ Part 1.3) OR The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~did not include incident handling procedures for Cyber Security Incidents. (~~Requirement R1~~ Part 1.4) OR The Responsible Entity's ~~has developed a Cyber Security Incident response~~ plan~~, but the plan does~~did not include one or more processes to provide notification per	The Responsible Entity ~~has~~ did not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (~~Requirement R1~~ Part 1.1) OR The Responsible Entity ~~has developed a Cyber Security Incident response plan, but the plan does~~did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the “Applicable Systems” column for Part 1.2. (~~Requirement R1~~ Part 1.2)

R #	**Violation Severity Levels (CIP-008-7)**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			Requirement R4. (~~Requirement R1~~ Part 1.2) OR The Responsible Entity ~~has developed a Cyber Security Incident response~~ plan~~, but the plan does~~did not include one or more processes that include criteria to evaluate and define attempts to compromise. (~~Requirement R1~~ Part 1.2)	
R2	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (~~Requirement R2~~ Part 2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (~~Requirement R2~~ Part 2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (~~Requirement R2~~ Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (~~Requirement R2~~ Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the ~~“~~Applicable

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			was an attempt to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column for Part 2.2 occurs. (~~Requirement R2~~ Part 2.2)	Systems~~”~~ column for Part 2.3. (~~Requirement R2~~ Part 2.3)
R3	The Responsible Entity ~~has~~ did not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (~~Requirement R3~~ Part 3.1.3)	The Responsible Entity ~~has~~did not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (~~Requirement R3~~ Part 3.1.2) OR The Responsible Entity ~~has~~ did not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the	The Responsible Entity ~~has~~ did neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (~~Requirement R3~~ Part 3.1.1) OR The Responsible Entity ~~has~~ did not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (~~Requirement R3~~ Part 3.1.1)

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-008-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td>Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (~~Requirement R3~~ Part 3.1.3)
OR
The Responsible Entity ~~has~~ did not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (~~Requirement R3~~ Part 3.2)
• Roles or responsibilities, or</td><td>Cyber Security Incident. (~~Requirement R3~~ Part 3.1.2)
OR
The Responsible Entity ~~has~~did not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (~~Requirement R3~~ Part 3.2)
• Roles or responsibilities, or
• Cyber Security Incident response groups or individuals, or
• Technology changes.</td><td></td></tr>
</table>

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		• Cyber Security Incident response groups or individuals, or • Technology changes.		
R4	The Responsible Entity did not notify~~ied~~ or update E-ISAC, ~~and~~or CISA, or their successors, ~~of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed to notify or update E-ISAC or CISA, or their successors, within the timeline~~s pursuant to Part 4.2. (~~Requirement R4~~ Part 4.2) OR The Responsible Entity ~~notified E-ISAC and CISA, or their~~	The Responsible Entity ~~failed to~~did not notify E-ISAC, or CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the ~~"~~Applicable Systems~~"~~ column. (~~Requirement R4~~ Part R4)	The Responsible Entity did not notifiy~~ed~~ E-ISAC, ~~and~~ or CISA, or their successors, ~~of a Reportable Cyber Security Incident but failed to notify or update E-ISAC or CISA, or their successors,~~ within the timelines pursuant to Part 4.2. (~~Requirement R4~~ Part 4.2) OR The Responsible Entity ~~failed to~~did not notify E-ISAC or CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	The Responsible Entity ~~failed to~~did not notify E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.3 but failed to~~did not report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (~~Requirement R4~~ Part 4.3) OR The Responsible Entity ~~notified E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an~~			

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to~~did not report on one or more of the attributes after determination pursuant to Part 4.1. (~~Requirement R4~~ Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See "Project 2016-02 Virtualization Implementation Plan."

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	

Version	Date	Action	Change Tracking
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	TBD	Modified to address directives in FERC Order No. 848	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 3 Definitions"

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7~~6~~

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the Bulk Electric System (BES):

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Remedial Action Scheme~~RAS where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-7~~6~~:

4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BES) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates:

See "Project 2016-02 Modifications to CIP Standards Implementation Plan"~~ for CIP-008-6~~.

~~**6. Background:**~~

~~Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

~~**High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~6~~7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~6~~ 7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ Electronic Access Control and Monitoring Systems (EACMS) Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the “Applicable Systems” column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “Applicable Systems” column including justification for attempt determination criteria and documented processes for notification.

CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.3	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. -Types of exercises may include discussion or operations based exercises.

CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.2	High ~~I~~impact~~ BES Cyber Systems~~BCS and their associated ~~:~~ EACMS Medium ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA)~~National Cybersecurity and Communications Integration Center (NCCIC)~~,~~[1]~~ or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the “Applicable Systems” column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column according to the applicable requirement parts in *CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS~~ BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and ~~NCCIC~~CISA, or their successors.

~~[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).~~

CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	After the Responsible Entity’s determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: - One hour after the determination of a Reportable Cyber Security Incident. - By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ~~NCCIC~~CISA, or their successors.

CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.3	High ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within ~~7~~ seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and ~~NCCIC~~CISA, or their successors.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~
- ~~Complaint~~

~~**Additional Compliance Information:**~~

~~None~~

2. Table of Compliance Elements

R #	Violation Severity Levels (CIP-008-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~ did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible Entity's ~~has developed a Cyber Security Incident response plan, but the~~ plan ~~does~~ did not include one or more processes to	The Responsible Entity ~~has~~ did not develop~~ed~~ a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible Entity's ~~has developed a Cyber Security Incident response plan, but the~~ plan ~~does~~did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the ~~“~~Applicable Systems~~”~~ column for Part 1.2. (Part 1.2)

			provide notification per Requirement R4. (Part 1.2) OR The Responsible Entity's ~~has developed a Cyber Security Incident response plan, but the~~ plan ~~does~~ did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	
R2	The Responsible Entity ~~has~~ did not test~~ed~~ the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Par 2.1)	The Responsible Entity ~~has~~did not test~~ed~~ the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity ~~has~~ did not test~~ed~~ the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column for Part 2.2 occurs. (Part 2.2)	The Responsible Entity ~~has~~ did not test~~ed~~ the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column for Part 2.3. (Part 2.3)

R3	The Responsible Entity ~~has~~did not notify~~ied~~ each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	The Responsible Entity ~~has~~did not update~~d~~ the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity ~~has~~ did not notify~~ied~~ each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1) OR The Responsible Entity ~~has~~ did not update~~d~~ the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity ~~has~~ did not update~~d~~ the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)

		The Responsible Entity ~~has~~ did not update~~d~~ the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	
R4	The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed~~ did not ~~to~~ notify	The Responsible Entity ~~failed to~~did not notify E-ISAC or ~~NCCIC~~CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system	The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to~~did not notify or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2)	The Responsible Entity ~~failed to~~ did not notify E-ISAC and ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

	or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.3 but failed to~~did not report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3) OR The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber~~	identified in the ~~“~~Applicable Systems~~”~~ column. (Requirement R4)	OR The Responsible Entity ~~failed to~~did not notify E-ISAC or ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	

	~~Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to~~ did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 3 Definitions".

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	Examples of evidence may include, but are not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover Applicable System functionality.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Examples of evidence may include, but are not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Examples of evidence may include, but are not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: - By recovering from an actual incident; - With a paper drill or tabletop exercise; or - With an operational exercise.	Examples of evidence may include, but are not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover Applicable System functionality substitutes for this test.	Examples of evidence may include, but are not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.	Examples of evidence may include, but are not limited to, dated documentation of: - An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
		An actual recovery response may substitute for an operational exercise.	• An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable Requirement Parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the Applicable Requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated:	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:	Examples of evidence may include, but are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS	3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:
As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:
The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information: None

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity's plan(s) did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity plan(s) did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity did not create recovery plan(s) for Applicable Systems. OR The Responsible Entity plan(s) did not address the conditions for activation in Part 1.1. OR The Responsible Entity plan(s) did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to	The Responsible Entity did not test the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 16 calendar months, not exceeding 17	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 17 calendar	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 18 calendar months between tests. (Part 2.2) OR

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)	calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)	months, not exceeding 18 calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)	The Responsible Entity did not test the recovery plan(s) according to Part 2.3 within 39 calendar months between tests of the plan(s). (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Part 3.1.3)	The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3)	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1) OR The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2)	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		OR The Responsible Entity did not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part 3.2)	OR The Responsible Entity did not update the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
~~45~~63-day formal comment period with ballot	June 30 – ~~August 13~~September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~August 3–September 16, 2021~~
Final Ballot	~~October 19–28, 2021~~April 2022
Board adoption	~~November 4, 2021~~May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. Generator Operator

    4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-009-7:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication network and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002-7 identification and categorization processes.

4.3. **“Applicable Systems” ~~Columns in Tables~~:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*.

CIP-009-7 Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.1	High ~~I~~impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS) PACS; and 2. Physical Access Control Systems (PACS) Medium ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS ~~SCI identified independently supporting an Applicable System above~~	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS ~~SCI identified independently supporting an Applicable System above~~	Roles and responsibilities of responders.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS ~~SCI identified independently supporting an Applicable System above~~	One or more processes for the backup and storage of information required to recover ~~a~~Applicable ~~s~~System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover ~~a~~Applicable ~~s~~System functionality.

CIP-009-7 Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.4	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS ~~SCI identified independently supporting an Applicable System above~~	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS SCI identified independently supporting an Applicable System ~~above~~in this Part	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BBCS at Control Centers and their associated: 1. EACMS; and 2. PACS ~~SCI hosting High or Medium Impact BCS at Control Centers or their associated:~~ ~~• PACS; or~~ ~~• EACMS~~ ~~SCI identified independently supporting an Applicable System above~~	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS ~~SCI hosting High or Medium Impact BCS at Control Centers or their associated:~~ - ~~PACS; or~~ - ~~EACMS~~ ~~SCI identified independently supporting an Applicable System above~~	Test a representative sample of information used to recover ~~a~~Applicable ~~s~~System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover applicable system functionality substitutes for this test.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BCS ~~SCI identified independently supporting an Applicable System above~~	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High Impact BCS and their associated: 1. EACMS; and 2. PACS Medium Impact BCS at Control Centers and their associated: 1. EACMS: and 2. PACS ~~SCI identified independently supporting an Applicable System above~~	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BSC at Control Centers and their associated: 1. EACMS; and 2. PACS ~~SCI identified independently supporting an Applicable System above~~	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	The Responsible Entity ~~has developed recovery plan(s), but the~~ plan(s) ~~do~~did not address one of the requirements included in Requirement R1 Parts 1.2 through 1.5.	The Responsible Entity ~~has developed recovery plan(s), but the~~ plan(s) ~~do~~ did not address two of the requirements included in ~~Requirement R1~~ Parts 1.2 through 1.5.	The Responsible Entity ~~has~~did not created recovery plan(s) for applicable systems. OR The Responsible Entity ~~has created recovery plan(s) for applicable systems, but the plan(s) does~~ did not address the conditions for activation in ~~Requirement R1~~ Part 1.1. OR The Responsible Entity ~~has created recovery plan(s) for applicable systems, but the plan(s) does~~did not address three or more of the requirements in Parts ~~Requirement R1~~1.2 through 1.5.
R2.	The Responsible Entity ~~has~~did not test~~ed~~ the recovery plan(s) according to ~~R2~~ Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s).	The Responsible Entity ~~has~~did not test~~ed~~ the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (~~Requirement R2~~ Part 2.1) OR	The Responsible Entity ~~has~~did not test~~ed~~ the recovery plan(s) according to ~~R2~~ Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (~~Requirement R2~~ Part 2.1)	The Responsible Entity ~~has~~did not test~~ed~~ the recovery plan(s) according to ~~R2~~ Part 2.1 within 18 calendar months between tests of the plan. (~~Requirement R2~~ Part 2.1) OR The Responsible Entity ~~has~~did not test~~ed~~ a representative sample of the information used in the recovery of Applicable System functionality

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	(~~Requirement R2~~ Part 2.1) OR The Responsible Entity ~~has~~did not test~~ed~~ a representative sample of the information used in the recovery of ~~a~~Applicable ~~s~~System functionality according to ~~R2~~ Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (~~Requirement R2~~ Part 2.2) OR The Responsible Entity ~~has~~did not test~~ed~~ the recovery plan according to ~~R2~~ Part 2.3 within 36 calendar months, not exceeding 37 calendar months between	The Responsible Entity ~~has~~did not tested a representative sample of the information used in the recovery of ~~a~~Applicable ~~s~~System functionality according to ~~R2~~ Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (~~Requirement R2~~ Part 2.2) OR The Responsible Entity ~~has~~did not test~~ed~~ the recovery plan according to ~~R2~~ Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (~~Requirement R2~~ Part 2.3)	OR The Responsible Entity ~~has~~did not test~~ed~~ a representative sample of the information used in the recovery of ~~a~~Applicable ~~s~~System functionality according to ~~R2~~ Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (~~Requirement R2~~ Part 2.2) OR The Responsible Entity ~~has~~did not test~~ed~~ the recovery plan according to ~~R2~~ Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (~~Requirement R2~~ Part 2.3)	according to R2 Part 2.2 within 18 calendar months between tests. (~~Requirement R2~~ Part 2.2) OR The Responsible Entity ~~has~~did not tested the recovery plan(s) according to ~~R2~~ Part 2.3 within 39 calendar months between tests of the plan. (~~Requirement R2~~ Part 2.3)

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	tests. (~~Requirement~~ R2 Part 2.3)			
R3.	The Responsible Entity ~~has~~did not notify~~ied~~ each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (~~Requirement R3~~ Part 3.1.3)	The Responsible Entity ~~has~~did not update~~d~~ the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (~~Requirement R3~~ Part 3.1.2) OR The Responsible Entity ~~has~~did not notify~~ied~~ each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (~~Requirement R3~~ Part 3.1.3) OR The Responsible Entity ~~has~~ did not update~~d~~ the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (~~Requirement R3~~ Part 3.1.1) OR The Responsible Entity ~~has~~did not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (~~Requirement R3~~ Part 3.1.2) OR	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (~~Requirement R3~~ Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		that the responsible entity determines would impact the ability to execute the plan: (~~Requirement R3~~ Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	The Responsible Entity ~~has~~did not update~~d~~ the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (Requirement R3 Part 3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

See “Project 2016-02 Modification to CIP Standards Implementation Plan.”

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	

Version	Date	Action	Change Tracking
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	TBD	Virtualization conforming changes	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 3 Definitions"

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7~~6~~

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~Interchange Coordinator or Interchange Authority~~

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System or Remedial Action Scheme~~RAS where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-009-7~~6~~:

4.2.3.1 Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **"Applicable Systems":** Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates:

See "Project 2016-02 Modifications to CIP Standards Implementation Plan" ~~for CIP-009-6~~.

~~**6. Background:**~~

~~Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a~~

~~program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~“Applicable Systems” Columns in Tables:~~

~~Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber~~

~~System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable ~~r~~Requirement ~~p~~Parts in *CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable ~~r~~Requirement ~~p~~Parts in *CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications*.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover ~~BES Cyber~~ Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover ~~BES Cyber~~Applicable System functionality.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per ~~Cyber Asset~~system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable ~~r~~Requirement ~~p~~Parts in *CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable ~~r~~Requirement ~~p~~Parts in *CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover ~~BES Cyber~~ Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover ~~BES Cyber~~Applicable System functionality substitutes for this test.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High ~~I~~impact BCS~~BES Cyber Systems~~	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable ~~r~~Requirement ~~p~~Parts in *CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the ~~a~~Applicable ~~r~~Requirement parts in *CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS ~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact -the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: - Emails; - USPS or other mail service; - Electronic distribution system; or - Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	N/A	The Responsible Entity's ~~has developed recovery plan(s), but the~~ plan(s) ~~do~~ did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity ~~has developed recovery plan(s), but the~~ plan(s) ~~do~~ did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity ~~has~~ did not create~~d~~ recovery plan(s) for ~~BES Cyber~~Applicable Systems. OR The Responsible Entity ~~has created recovery plan(s) for BES Cyber Systems, but the~~ plan(s) ~~does~~ did not address the conditions for activation in Part 1.1. OR The Responsible Entity ~~has created recovery plan(s) for BES Cyber Systems, but the~~ plan(s) ~~does~~ did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan(s) according to ~~R2~~ Part 2.1 within 15 calendar months, not exceeding 16 calendar months	The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1)	The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan(s) according to ~~R2~~ Part 2.1 within 17 calendar months, not exceeding 18 calendar months between	The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan(s) according to ~~R2~~ Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	between tests of the plan(s). (Part 2.1) OR The Responsible Entity ~~has~~ did not test~~ed~~ a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not test~~ed~~ the recovery plan according to ~~R2~~ Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)	OR The Responsible Entity ~~has~~ did not test~~ed~~ a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan according to ~~R2~~ Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)	tests of the plan. (Part 2.1) OR The Responsible Entity ~~has~~ did not test~~ed~~ a representative sample of the information used in the recovery of ~~BES Cyber~~ Applicable System functionality according to ~~R2~~ Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan according to ~~R2~~ Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)	The Responsible Entity ~~has~~ did not test~~ed~~ a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 18 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan(s) according to ~~R2~~ Part 2.3 within 39 calendar months between tests of the plan(s). (Part 2.3)
R3	The Responsible Entity ~~has~~ did not notify~~ied~~ each person or group	The Responsible Entity ~~has~~ did not update~~d~~ the recovery plan(s) based on	The Responsible Entity ~~has~~ neither documented lessons learned nor	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Part 3.1.3)	any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity ~~has~~ did not notify~~ied~~ each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3) OR The Responsible Entity ~~has~~ did not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact	documented the absence of any lessons learned within 90 and less than 120 calendar days ~~-~~of each recovery plan test or actual recovery. (Part 3.1.1) OR The Responsible Entity ~~has~~ did not update~~d~~ the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity ~~has~~ did not update~~d~~ the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact	absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Responders, or • Technology changes. (Part 3.2)	the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~The following guidelines are available to assist in addressing the required components of a recovery plan:~~

- ~~NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf~~
- ~~National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf~~

~~The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.~~

~~A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.~~

~~For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.~~

~~For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.~~

~~For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:~~

1. ~~Installation files and media;~~
2. ~~Current backup tapes and any additional documented configuration settings;~~
3. ~~Documented build or restoration procedures; and~~
4. ~~Cross site replication storage.~~

~~For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:~~

- ~~Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.~~
- ~~Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.~~
- ~~Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.~~
- ~~Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.~~

~~The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.~~

~~For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.~~

~~Requirement R2:~~

~~A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.~~

~~A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.~~

~~Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."~~

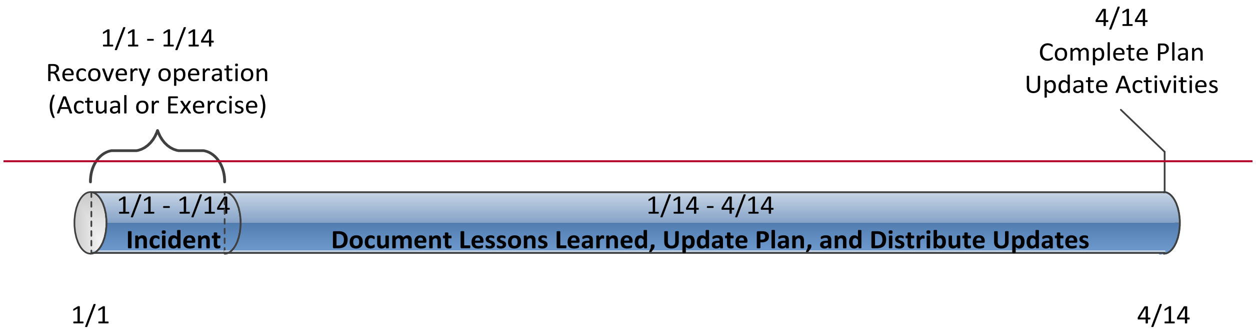
~~The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."~~

~~For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.~~

~~**Requirement R3:**~~

~~This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.~~

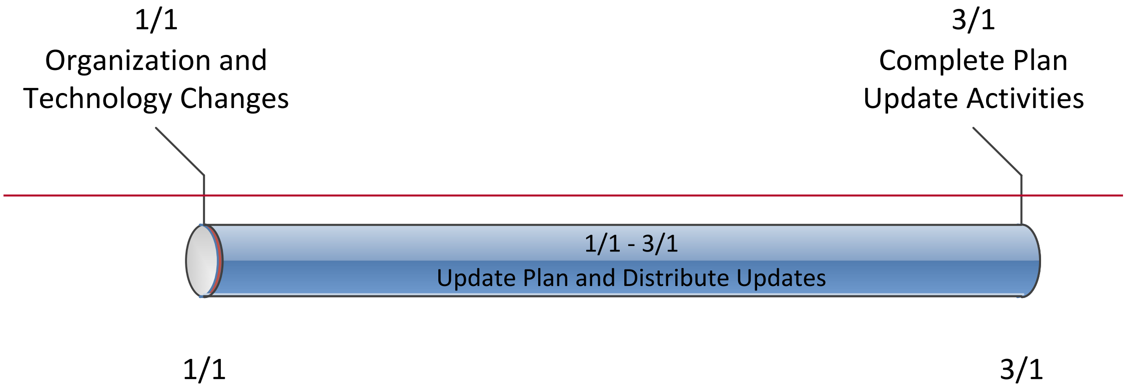
~~The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.~~



~~**Figure 1: CIP-009-6 R3 Timeline**~~

~~The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.~~

~~The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.~~



~~**Figure 2: Timeline for Plan Changes in 3.2**~~

~~When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.~~

~~Rationale for Requirement R2:~~

~~The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.~~

~~Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.~~

~~Rationale for Requirement R3:~~

~~To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled “Project 2016-02 Draft 3 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Define types of changes that may impact CIP-005 or CIP-007 security controls. For those changes: 1.1.1. Prior to change implementation, identify impacted security controls in CIP-005 and CIP-007, except during CIP Exceptional Circumstances; 1.1.2. Authorize those changes; and 1.1.3. Verify cyber security controls from CIP-005 and CIP-007 are not adversely affected.	Examples of evidence may include, but are not limited to, a documented process that defines changes that may impact security controls in CIP-005 and CIP-007, such as but not limited to: • Operating system (OS) software; • Firmware, where no independent OS exists; • Commercially available or open-source application software, including application containers; • Custom software installed, including application containers; • Configuration that modifies network accessible logical ports or network accessible services on an Applicable System; • SCI configuration of host affinity control between systems with different impact ratings; • Changes to configurations or settings

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			for an ESP between systems with different impact ratings; • Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations; or • Any other configuration or setting determined by the Responsible Entity. (1.1.1.) • Documentation of the impacted security controls in CIP-005 and CIP-007; (1.1.2.) • A change request record and associated authorization for applicable changes; or • Records from a change management system that identifies applicable changes and records of authorization for changes. (1.1.3.) • A list of cyber security controls verified or tested along with the dated test results; or • An output from cyber security testing tools such as a vulnerability scanner.
1.2	High impact BCS	1.2.1. Prior to implementing any change in the production environment, except	An example of evidence may include, but is not limited to, a list of cyber security

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part Note: Implementation does not require the Responsible Entity to renegotiate or	Prior to software (or firmware where no OS exists) version change and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.		

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Methods to monitor for unauthorized changes at least once every 35 calendar days. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring for unauthorized changes along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BES Cyber Systems SCI supporting an Applicable System in this Part	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements of the same type of Cyber Systems with a configuration of the previous or other existing Cyber System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of any tools used to perform the assessment, or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.
3.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of evidence may include, but are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets and SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCA(s) or Removable Media*.*

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's change management process(es) did not include one of the required items listed in 1.1.1 through 1.1.3. (Part 1.1)	The Responsible Entity's change management process(es) did not define the types of changes that may impact either CIP-005 or CIP-007 controls. (Part 1.1) OR The Responsible Entity's change management process(es) does not include two of the required items listed in 1.1.1 through 1.1.3. (Part 1.1); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity's management process(es) did not define the types of changes that may impact both CIP-005 and CIP-007 controls. (Part 1.1) OR The Responsible Entity change management process(es) did not include the three required items listed in 1.1.1 through 1.1.3. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. (Part 1.2); OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity neither documented nor implemented any change management process(es) that include required items in Part 1.1 through Part 1.3. (Requirement R1)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	N/A	N/A	The Responsible Entity did not document nor implemented a process(es) with methods to monitor for unauthorized changes at least once every 35 calendar days. (Part 2.1); OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1);	The Responsible Entity neither documented nor implemented a process(es) with methods to monitor for at least once every 35 calendar days and neither documented nor investigated detected unauthorized changes. (Part 2.1)
R3.	The Responsible Entity performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity did not implement any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3) OR The Responsible Entity performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity performed an active

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2) OR The Responsible Entity did not perform the active vulnerability assessment of a Cyber System prior to it becoming an Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	The Responsible Entity did not manage its Transient Cyber Asset(s) according to Attachment 1, Section 1.1. (Requirement R4) OR The Responsible Entity did not document the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document authorization for TCA managed by the Responsible Entity according to Attachment 1, Section 1.2. (Requirement R4)	The Responsible Entity did not implement the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCA managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4)	The Responsible Entity did not authorize its TCA(s) according to Attachment 1, Section 1.2. (R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	The Responsible Entity did not document or implement one or more plan(s) for TCAs and Removable Media according to Requirement R4. (Requirement R4)

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.
- CIP-010-5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	

CIP-010-5 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCA(s). This can be included as part of the TCA(s), part of the documentation related to authorization of TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, methods to maintain the known good state of the OS and all software, or system hardening practices. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, controls to maintain the known good state of the OS and all software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic

mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, controls to maintain the known good state of the OS and all software by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~second~~ third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
~~45~~63-day formal comment period with ballot	June 30 – ~~August 13~~September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~August 29–October 11, 2021~~
Final Ballot	~~October 19–28, 2021~~April 2022
Board adoption	~~November 4, 2021~~May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security —Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting ~~BES Cyber Systems~~BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1. Balancing Authority

      4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

            4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

      4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communications links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems” ~~**Columns in Tables**~~**:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented ~~change management~~ process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact BES Cyber Systems (BCS) and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI~~ identified independently~~ supporting an Applicable System ~~above~~in this Part	~~Authorize~~ Define types of changes that may impact CIP-005 or CIP-007 security controls. For those changes~~ to~~: 1.1.1. Prior to change implementation, identify impacted security controls in CIP-005 and CIP-007, except during CIP Exceptional Circumstances~~Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems; or firmware~~; 1.1.2. ~~Commercially available or open-source application software, including application containers~~Authorize those changes~~-~~; 1.1.3. ~~Custom software installed, including applications containers; and~~Verify cyber	Examples of evidence may include, but are not limited to, a documented process that defines changes that may impact security controls in CIP-005 and CIP-007, such as but not limited to: • Operating system (OS) software; • Firmware, where no independent OS exists; • Commercially available or open-source application software, including application containers; • Custom software installed, including application containers; • Configuration that modifies network accessible logical ports or network accessible services on an Applicable System; • SCI configuration of host affinity control between systems with

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		security controls from CIP-005 and CIP-007 are not adversely affected. ~~Any logical network accessible ports (or services if unable to determine ports).~~	different impact ratings; • Changes to configurations or settings for an ESP between systems with different impact ratings; • Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) • Any other configuration or setting determined by the Responsible Entity. (1.1.1.) • Documentation of the impacted security controls in CIP-005 and CIP-007; (1.1.2.) • A change request record and associated authorization for applicable changes; or • Records from a change management system that identifies applicable changes and records of authorization for changes. (1.1.3.) • A list of cyber security controls verified or tested along with the

CIP-010-5 Table R1 – ~~Configuration~~ Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			dated test results; or • An output from cyber security testing tools such as a vulnerability scanner. • ~~• A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change.~~ ~~• Documentation of authorization for cyber security patch implementation.~~
1.2	~~SCI identified independently supporting an Applicable System from Part 1.1.~~High Impact BCS	~~Authorize changes to SCI configuration that:~~ ~~1.2.1. Controls sharing of CPU or memory between systems with different impact ratings, including non-CIP Systems, hosted on SCI; and~~ ~~1.2.2. Enforces an ESP between systems with different impact ratings, including non-CIP Systems, hosted on SCI.~~	An ~~E~~example~~s~~ of evidence may include, but ~~are~~is not limited to,~~:~~ a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test. ~~• Documentation of authorization for changes to configuration of~~

CIP-010-5 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
		~~1.2.3.~~1.2.1. Prior to implementing any change in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	~~host affinity control between systems with different impact ratings;~~ • ~~Documentation of authorization for changes to policies or configurations for an ESP between systems with different impact ratings.~~
1.3	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS~~; and~~	~~For each change to the items listed in Part 1.1:~~ ~~1.3.1.~~ Prior to softare (or firmware	An example of evidence may include, but is not limited to, a change request record that demonstrates the verification of identity of the software

CIP-010-5 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	~~PCA~~ Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS~~; and~~ ~~PCA~~ SCI~~ identified independently~~ supporting an Applicable System ~~above~~in this Part Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	where no OS exists) version change and when the method to do so is available to the Responsible Entity from the software source: ~~the change, except during CIP Exceptional Circumstances, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change~~; 1.3.1~~2~~.~~ Following the change, v~~Verify ~~that required cyber security controls determined in 1.3.1 are not adversely affected~~the identity of the software sources; and 1.~~3~~2~~.~~.3. ~~Document the results of the verification~~Verify the integrity of the software obtained from the software source.	source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.~~a list of cyber security controls verified or tested along with the dated test results.~~
~~1.4~~	~~High Impact BCS~~ ~~SCI identified independently supporting an Applicable System above~~	~~For each change to the items listed in Part 1.1 or Part 1.2, per system capability:~~ ~~1.4.1. Prior to implementing any change in the production environment, except during a CIP Exceptional Circumstance, test the~~	~~An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences~~

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		~~changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and~~ ~~1.4.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.~~	~~were accounted for, including the date of the test.~~
~~**1.5**~~	~~High Impact BCS and their associated:~~ ~~1. EACMS; and~~ ~~2. PACS~~ ~~Medium Impact BCS and their associated:~~ ~~1. EACMS; and~~ ~~2. PACS~~ ~~SCI identified independently~~	~~Prior to a change associated with Parts 1.1.1 and 1.1.2 and when the method to do so is available to the Responsible Entity from the software source:~~ ~~1.5.1. Verify the identity of the software source; and~~ ~~1.5.2. Verify the integrity of the software obtained from the software source.~~	~~An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the~~

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~supporting an Applicable System above~~ ~~Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.5: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.~~		~~software.~~

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – ~~Change~~ Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Change Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – ~~Change~~ Configuration Monitoring

Part	Applicable Systems	Requirements	Measures
2.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Methods to ~~M~~monitor ~~at least once every 35 calendar days for unauthorized changes to the items listed in Requirement R1, Part 1.1. and Part 1.2. Document and investigate detected~~for unauthorized changes at least once every 35 calendar days. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.1	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI i~~dentified independently~~ supporting an Applicable System ~~above~~in this Part	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~I~~impact BES Cyber Systems SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: - like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System; or - CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: - The output of any tools used to perform the assessment, or - Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.

CIP-010-5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.4	High ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to: • Reports or logs from ~~SCI~~ automated mechanisms ~~and~~ that perform remediation of VCAs at instantiation; or • Documention listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high and medium impact BCSand associated PCA and SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1~~, except for use on low impact BCS or SCI supporting only low impact BCS(s)~~. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCAs and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCAs or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCAs or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's ~~has documented and implemented a~~ change management ~~authorization~~ process(es) did not ~~that~~ include~~s only four or more~~ one of the required items listed in 1.1.1 through 1.1.4. (~~Requirement R1~~ Part 1.1)	The Responsible Entity's ~~has documented and implemented a~~ change management ~~authorization~~ process(es) did not define the types of changes that may impact either CIP-005 or CIP-007 controls. ~~includes only three of the required items listed in 1.1.1 through 1.1.4.~~ (~~Requirement R1~~ Part 1.1) OR The Responsible Entity's change management process(es) does not include two of the required items listed in 1.1.1 through 1.1.3. (Part 1.1); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Part 1.2);	The Responsible Entity's ~~has documented and implemented a change authorization~~management process(es) did not define the types of change that may impact both CIP-005 and CIP-007 controls. ~~that includes only two of the required items listed in 1.1.1 through 1.1.4.~~ (~~Requirement R1~~ Part 1.1) OR The Responsible Entity change management process(es) did not include the three required items listed in 1.1.1 through 1.1.3. (Part 1.1) OR The Responsible Entity's ~~has documented and implemented a~~ change management ~~authorization~~ process(es) ~~that~~does not include~~s only one of~~ the two	The Responsible Entity ~~has not~~neither documented nor implemented any change ~~authorization~~ management process(es) in Part 1.1 through Part 1.3. (Requirement R1) ~~OR~~ ~~The Responsible Entity has documented and implemented a change authorization process(es) that includes only one of the required items listed in 1.1.1 through 1.1.4. (Requirement R1 Part 1.1)~~ ~~OR~~ ~~The Responsible Entity does not have a change authorization process(es) that requires authorization of changes to items listed in 1.1.1-1.1.4. (Requirement R1 Par~~t ~~1.1)~~ ~~OR~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	required items listed in 1.2.1 through 1.2.2. (~~Requirement R1~~ Part 1.2) OR The Responsible Entity's ~~has a process as specified in Part 1.5 to verify the identity of the software source (1.5.1) but does not have a~~change management process(es) ~~as specified in Part 1.5 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source~~does not include the two required items listed in 1.3.1 through 1.3.2. (~~Requirement R1~~ Part 1.~~5.2~~3)	~~The Responsible Entity does not have a change authorization process(es) that requires authorization of changes to items listed in 1.2.1 to 1.2.2 (Requirement R1 Part 1.2)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing configuration. (Requirement R1 Part 1.3.1)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing configuration but did not verify and document that the required controls were not adversely~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~affected following the change. (Requirement R1 Part 1.3.2 & Part 1.3.3)~~ ~~OR~~ ~~The Responsible Entity does not have a process for testing changes prior to implementing a change tothe configuration. (Requirement R1 Part 1.4.1)~~ ~~OR~~ ~~The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (Requirement R1 Part 1.4.2)~~ ~~OR~~ ~~The Responsible Entity does not have a process as specified in Part 1.5 to verify the identity of the software source and the integrity of the software provided by~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~the software source when the method to do so is available to the Responsible Entity from the software source. (Requirement R1 Part 1.5)~~
R2.	N/A	N/A	~~N/A~~ The Responsible Entity did not document nor implemented a process(es) with methods to monitor for unauthorized changes at least once every 35 calendar days. (Part 2.1); OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1);	The Responsible Entity ~~has not~~neither documented nor implemented a process(es) ~~to~~ with methods to monitor for at least once every 35 calendar days and neither~~,~~ ~~investigate, and~~ document nor investigated detected unauthorized changes.~~ to the items described in Requirement R1, Part 1.1. at least once every 35 calendar days.~~ (~~Requirement R2~~ Part 2.1) ~~OR~~ ~~The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the items described in~~

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				~~Requirement R1, Part 1.2. at least once every 35 calendar days. (Requirement R2 Part 2.1)~~
R3.	The Responsible Entity ~~has implemented one or more documented~~performed a vulnerability assessment ~~processes for each of its Applicable Systems, but has performed a vulnerability assessment~~ more than 15 months, ~~but less than 18 months,~~ since the last assessment on one of its Applicable Systems. (~~Requirement R3~~ Part 3.1) OR The Responsible Entity ~~has implemented one or more documented~~performed an active vulnerability assessment ~~processes for Applicable Systems, but has performed an active vulnerability assessment~~ more than 36 months, but less than 39 months, since	The Responsible Entity ~~has implemented one or more documented~~ performed a vulnerability assessment ~~processes for each of its Applicable Systems, but has performed a vulnerability assessment~~ more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (~~Requirement R3~~ Part 3.1) OR The Responsible Entity ~~has implemented one or more documented~~ performed an active vulnerability assessment ~~processes for Applicable Systems, but has performed an active vulnerability assessment~~ more than 39 months, but less than 42 months, since	The Responsible Entity ~~has implemented one or more documented~~an active vulnerability assessment ~~processes for each of its Applicable Systems, but has performed a vulnerability assessment~~ more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (~~Requirement R3~~ Part 3.1) OR The Responsible Entity ~~has implemented one or more documented~~ performed an active vulnerability assessment ~~processes for Applicable Systems, but has performed an active vulnerability assessment~~ more than 42 months, but less than 45 months, since	The Responsible Entity ~~has~~did not implemented any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3) OR The Responsible Entity ~~has implemented one or more documented~~performed a vulnerability assessment ~~processes for each of its Applicable Systems, but has performed a vulnerability assessment~~ more than 24 months since the last assessment on one of its applicable BES Cyber systems. (~~Requirement R3~~ Part 3.1) OR The Responsible Entity has ~~implemented one or more~~

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	the last active assessment on one of its Applicable Systems. (~~Requirement R3~~ Part 3.2)	the last active assessment on one of its Applicable Systems. (~~Requirement R3~~ Part 3.2)	the last active assessment on one of its Applicable Systems. (~~Requirement R3~~ Part 3.2)	~~documented~~performed an active vulnerability assessment ~~processes for Applicable Systems, but has performed an active vulnerability assessment~~ more than 45 months since the last active assessment on one of its applicable BES Cyber ~~s~~Systems.(~~Requirement R3~~ Part 3.2) OR The Responsible Entity ~~has implemented and documented one or more vulnerability assessment processes for each of its Applicable Systems, but~~ did not perform the active vulnerability assessment of a Cyber System prior to it becoming an Applicable System. (~~Requirement~~ R3 Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessment processes for each of its Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (~~Requirement R3~~ Part 3.4)
R4.	The Responsible Entity ~~documented its plan(s) for~~did not ~~TCAs and Removable Media, but failed to~~ manage its TCA(s) according to CIP-010-5, Requirement R4, Attachment 1, Section 1.1. (~~Requirement R4~~ Part R4) OR The Responsible Entity ~~documented its plan(s) for TCAs and Removable Media,~~	The Responsible Entity ~~documented its plan(s) for TCAs and Removable Media, but failed to~~did not implement the Removable Media sections according to CIP-010-5, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for TCAs and Removable Media~~	The Responsible Entity ~~documented its plan(s) for TCAs and Removable Media, but failed to~~did not authorize its TCA(s) according to CIP-010-5, Requirement R4, Attachment 1, Section 1.2. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for TCAs and Removable Media,~~	The Responsible Entity ~~failed to~~did not document or implement one or more plan(s) for TCAs and Removable Media according to CIP-010-5, Requirement R4. (Requirement R4)

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	~~but failed to~~did not document the Removable Media sections according to CIP-010-5, Requirement R4, Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for TCAs and Removable Media, but failed to~~did not document authorization for TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Section 1.2. (Requirement R4)	~~plan, but failed to~~did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity d~~ocumented its plan(s) for TCAs and Removable Media, but failed to~~did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections	~~but failed to~~did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for TCAs and Removable Media, but failed to~~ did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to CIP-010-5, Requirement R4, Attachment 1, Sections	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		2.1, 2.2, and 2.3. (Requirement R4)	2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See "Project 2016-02 Modifications to CIP Standards Implementation Plan.".
- CIP-010-5 Technical Rationale

CIP-010-5 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for ~~Transient Cyber Assets (~~TCA~~)~~ and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCA(s). This can be included as part of the TCA plan(s), part of the documentation related to authorization of TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, controls to maintain the known good state of the OS and all software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with controls to maintain the known good state of the OS and all software. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, controls to maintain the known good state of the OS and all software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, controls to maintain the known good state of the OS and all software by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/18	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	

Version	Date	Action	Change Tracking
4	TBD	Modified to address directives in FERC Order No. 850.	
5	TBD	Virtualization modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-54

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting ~~BES Cyber Systems~~BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5~~4~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~**4.2.3.2.**~~**4.2.3.3.** Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan” ~~for Project 2019-03~~.

~~6.~~ ~~**Background:** Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, “*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*” The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~

- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-54 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-54 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-54 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact BCS~~ES Cyber Systems~~ and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~I~~impact BCS~~ES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Define types of changes that may impact CIP-005 or CIP-007 security controls. ~~velop a baseline configuration, individually or by group, which shall include the following item~~For those changes: 1.1.1. Prior to change implementation, identify impacted security controls in CIP-005 and CIP-007, except during CIP Exceptional Circumstances~~Operating system(s) (including version) or firmware where no independent operating system exists~~; 1.1.2. Authorize those changes~~Any commercially available or open-source application software (including version) intentionally installed~~; and	Examples of evidence may include, but are not limited to, a documented process that defines changes that may impact security controls in CIP-005 and CIP-007, such as but not limited to: • Operating system (OS) software; • Firmware, where no independent OS exists; • Commercially available or open-source application software, including application containers; • Custom software installed, including application containers; • Configuration that modifies network accessible logical ports or network accessible services on an Applicable System; • SCI configuration of host affinity

CIP-010-54 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		1.1.3. Verify cyber security controls from CIP-005 and CIP-007 are not adversely affected~~Any custom software installed;~~ ~~1.1.4. Any logical network accessible ports; and~~ ~~1.1.5. Any security patches applied~~.	control between systems with different impact ratings; • Changes to configurations or settings for an ESP between systems with different impact ratings; • Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations; or • Any other configuration or setting determined by the Responsible Entity. (1.1.1.) • Documentation of the impacted security controls in CIP-005 and CIP-007; (1.1.2.) • A change request record and associated authorization for applicable changes; or • Records from a change management system that identifies applicable changes and records of authorization for changes. (1.1.3.)

CIP-010-~~5~~4 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			- A list of cyber security controls verified or tested along with the dated test results; or - An output from cyber security testing tools such as a vulnerability scanner. - ~~A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or~~ - ~~A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.~~
~~**1.2**~~	~~High Impact BES Cyber Systems and their associated:~~ ~~EACMS;~~ ~~1. PACS; and~~ ~~1. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~0. EACMS;~~ ~~0. PACS; and~~ ~~0. PCA~~	~~Authorize and document changes that deviate from the existing baseline configuration.~~	~~Examples of evidence may include, but are not limited to:~~ - ~~A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or~~ - ~~Documentation that the change was~~

CIP-010-5~~4~~ Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			~~performed in accordance with the requirement.~~
~~**1.3**~~	~~High Impact BES Cyber Systems and their associated:~~ ~~0. EACMS;~~ ~~0. PACS; and~~ ~~0. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.~~	~~An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.~~
~~**1.4**~~	~~High Impact BES Cyber Systems and their associated:~~ ~~0. EACMS;~~ ~~0. PACS; and~~ ~~0. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~0. EACMS;~~ ~~0. PACS; and~~ ~~0. PCA~~	~~For a change that deviates from the existing baseline configuration:~~ ~~1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;~~ ~~1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and~~ ~~1.4.3. Document the results of the verification.~~	~~An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.~~

CIP-010-54 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.2~~5~~	High ~~I~~impact BCS~~ES Cyber Systems~~	~~Where technically feasible, for each change that deviates from the existing baseline configuration:~~ 1.2~~5~~.1. Prior to implementing any change in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects~~, that models the baseline configuration~~ to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.2~~5~~.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-5~~4~~ Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3~~6~~	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to software (or firmware where no OS exists)~~a~~ version change ~~that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5,~~ and when the method to do so is available to the Responsible Entity from the software source: 1.3~~6~~.1. Verify the identity of the software source; and 1.3~~6~~.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5~~4~~ Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5~~4~~ Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5~~4~~ Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Methods to ~~M~~monitor for unauthorized changes at least once every 35 calendar days. ~~for changes to the baseline configuration (as described in Requirement R1, Part 1.1).~~ Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring ~~the configuration~~for unauthorized changes along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5~~3~~ Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5~~3~~ Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5~~4~~ Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-54 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~I~~impact BES Cyber Systems SCI supporting an Applicable System in this Part	~~Where technically feasible, a~~At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects~~, that models the baseline configuration of the BES Cyber System in a production environment~~; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-5~~4~~ Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: - Like replacements of the same type of Cyber Systems with a configuration of the previous or other existing Cyber System; or - CIP Exceptional Circumstances. ~~adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.~~	An example of evidence may include, but is not limited to: - The output of any tools used to perform the assessment, or - Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) ~~, a~~that documents ~~listing~~ the date of the assessment performed prior to becoming a new Applicable System. ~~the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.~~

CIP-010-5~~4~~ Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • ~~, a d~~Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets and SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for ~~Transient Cyber Assets~~TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for ~~Transient Cyber Assets~~TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use ~~Transient Cyber Asset~~TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use ~~Transient Cyber Asset~~TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's ~~has documented and implemented a configuration~~ change management process(es) did not~~that~~ include~~s~~ ~~only four~~ one of the required ~~baseline~~ items listed in 1.1.1 through 1.1.3~~5~~. (Part 1.1)	The Responsible Entity's ~~has documented and implemented a configuration~~ change management process(es) did not define the types of changes that may impact either CIP-005 or CIP-007 controls.~~that includes only three of the required baseline items listed in 1.1.1 through 1.1.5.~~ (Part 1.1) OR The Responsible Entity's change management process(es) does not include two of the required items listed in 1.1.1 through 1.1.3. (Part 1.1); OR The Responsible Entity's change management process(es) does not include one of the required items	The Responsible Entity's ~~has documented and implemented a configuration change~~ management process(es) did not define the types of changes that may impact both CIP-005 and CIP-007 controls. ~~that includes only two of the required baseline items listed in 1.1.1 through 1.1.5.~~ (Part 1.1) OR The Responsible Entity ~~has~~ change management ~~a~~ process(es) did not include the three required items listed in 1.1.1 through 1.1.3. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items	The Responsible Entity ~~has not~~neither documented nor implemented any ~~configuration~~ change management process(es) that include required items in Part 1.1 through Part 1.3. (Requirement R1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	listed in 1.2.1 through 1.2.2. (Part 1.2); OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) ~~as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)~~	~~existing baseline configuration. (1.2)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a~~

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td></td><td>~~change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)~~
~~OR~~
~~The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1)~~
~~OR~~
~~The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)~~</td></tr>
</table>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~OR~~ ~~The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)~~
R2.	N/A	N/A	The Responsible Entity did not document nor implemented a process(es) with methods to monitor for unauthorized changes at least once every 35 calendar days. (Part 2.1); OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1);~~N/A~~	The Responsible Entity ~~has not~~ neither documented nor implemented a process(es) with methods to monitor for, i~~nvestigate, and document detected unauthorized changes to the baseline~~ at least once every 35 calendar days and neither documented nor investigated detected unauthorized changes. (Part 2.1)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its ~~a~~Applicable Systems ~~BES Cyber Systems~~. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.2)	The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.2)	The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.2)	The Responsible Entity ~~has~~ did not implement~~ed~~ any vulnerability assessment processes for one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Requirement R3) OR The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2) OR The Responsible Entity ~~has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but~~ did not perform the active vulnerability assessment ~~in a manner that models an existing baseline configuration of its~~of a Cyber System prior to it becoming an ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				each of its ~~a~~Applicable ~~BES Cyber~~ Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)
R4.	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not manage its Transient Cyber Asset(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.1. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~ did not implement the Removable Media sections according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not authorize its ~~Transient Cyber Asset~~TCA(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity did not ~~failed to~~ document or implement one or more plan(s) for ~~Transient Cyber Assets~~TCAs and Removable Media according to ~~CIP-010-4,~~ Requirement R4. (Requirement R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Removable Media, but failed to~~did not document the Removable Media sections according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document authorization for ~~Transient Cyber Assets~~ TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (Requirement R4)	~~Removable Media plan, but failed to~~did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~ did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according	~~Removable Media, but failed to~~ did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCAs managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for ~~Transient Cyber Assets~~TCAs managed by a party other than the Responsible Entity according	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections ~~2.~~1.3, ~~2.2~~1.4, and ~~2.3.~~1.5. (Requirement R4)	to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan”~~ for Project 2019-03~~.
- CIP-010-54 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. ~~Transient Cyber Asset~~TCA(s) Managed by the Responsible Entity.

1.1. ~~Transient Cyber Asset~~TCA Management: Responsible Entities shall manage ~~Transient Cyber Asset~~TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, ~~to a BES Cyber System,~~ or (3) a combination of both (1) and (2) above.

1.2. ~~Transient Cyber Asset~~TCA Authorization: For each individual or group of ~~Transient Cyber Asset~~TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset~~TCA (per ~~Transient Cyber Asset~~TCA capability):

- Security patching, including manual or managed updates;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;
- ~~Live operating system and software executable only from read-only media;~~
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;

- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of ~~Transient Cyber Asset~~TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. ~~Transient Cyber Asset~~TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset~~TCA (per TCA~~Transient Cyber Asset~~ capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of ~~O~~other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code~~use of live operating system and software executable only from read-only media~~;
- Review of system hardening used by the party; or
- Review of ~~O~~other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset~~TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code ~~to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets~~, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ~~using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets~~; and

3.2.2. Mitigate the threat of detected malicious code ~~on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets~~.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the ~~Transient Cyber Asset~~TCA(s). This can be included as part of the ~~Transient Cyber Asset plan~~TCA(s), part of the documentation related to authorization of ~~Transient Cyber Asset~~TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of ~~Transient Cyber Asset~~TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, ~~or procedures or processes associated with~~methods to maintain the known good state of the OS and all software, or system hardening practices. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, controls to maintain the known good state of the OS and all software~~processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code~~, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, controls to maintain the known good state of the OS and all software ~~use of live of operating systems or system hardening performed~~ by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 3 Definitions"

A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-4
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 **Balancing Authority**

   4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 **Generator Operator**

   4.1.4 **Generator Owner**

   4.1.5 **Reliability Coordinator**

   4.1.6 **Transmission Operator**

   4.1.7 **Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers:**
All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-011-4:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards" Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BCSI pertaining to Applicable Systems identified in *CIP-011-4 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s).

CIP-011-4 Table R1 – Information Protection Program			
Part	Applicable Systems	Requirements	Measures
			Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-4 Table R2 –Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4 Table R2 –Reuse and Disposal

Part	Applicable Systems	Requirements	Measures
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).	Examples of evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

B. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-011-4)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not implement one or more BCSI protection program(s). (Requirement R1) OR The Responsible Entity did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity did not include disposal processes to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity neither documented nor implemented any processes for applicable requirement parts in CIP-011-4 Table R2 –Reuse and Disposal. (Requirement R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
~~45~~63-day formal comment period with ballot	June 30 – ~~August 13~~September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2021

Anticipated Actions	Date
~~45-day formal comment period with ballot~~	~~August 29– October 11, 2021~~
Final Ballot	~~October 19–28, 2021~~April 2022
Board adoption	~~November 4, 2021~~May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-4~~Y~~

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-~~Y~~4:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

5. **"Applicable Systems"~~ Columns in Tables~~:** Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

6. **Effective Dates:** See Project 2016-02 "Modification to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for ~~BES Cyber System Information (~~BCSI~~)~~ pertaining to "Applicable Systems" identified in *CIP-011-4~~Y~~ Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-4~~Y~~ Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-4~~Y~~ Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~Y~~4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact ~~BES Cyber Systems (~~BCS~~)~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Method(s) to identify BCSI.	Examples of evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.

CIP-011- ~~Y~~4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premises BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premises BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or

CIP-011-~~Y~~4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-4~~Y~~ Table R2 –Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4~~Y~~ Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4~~Y~~ Table R2 –Reuse and Disposal

Part	Applicable Systems	Requirements	Measures
2.1	High ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI ~~identified independently~~ supporting an Applicable System ~~above~~in this Part	Method(s) to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the ~~“~~Applicable Systems~~”~~ column).	Examples of evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

B. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-Y~~X~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A	N/A	The Responsible Entity ~~documented, but~~ did not~~,~~ implement one or more BCSI protection program(s). (Requirement R1); OR The Responsible Entity ~~documented but~~ did not implement at least one method to identify BCSI. (Part 1.1); OR The Responsible Entity ~~documented but~~ did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-Y~~X~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity ~~implemented one or more documented processes but~~ did not include processes for reuse ~~as~~ to prevent the unauthorized retrieval of BCSI from ~~the~~ an Applicable System~~BES Cyber Asset~~. ~~-~~(Part 2.1)	The Responsible Entity ~~implemented one or more documented processes but~~ did not include disposal ~~or media destruction~~ processes to prevent the unauthorized retrieval of BCSI from ~~the~~ an ~~BES Cyber Asset~~Applicable System. ~~-~~(Part 2.1~~2~~)	The Responsible Entity ~~has~~ neither~~not~~ documented nor implemented any processes for applicable R~~r~~equirement P~~p~~arts in CIP-011-4~~X~~ Table R2~~3~~ – BES Cyber Asset Reuse and Disposal. (Requirement R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	TBD	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-4~~3~~

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-4~~3~~:

4.2.3.1 Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~ 5.1a7~~ identification and categorization processes.

4.3. **"Applicable Systems":** Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards" Implementation Plan ~~for CIP-011-3~~.

~~6. **Background:** Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~“Applicable Systems” Columns in Tables:~~

~~Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for ~~BES Cyber System Information (~~BCSI~~)~~ pertaining to ~~“~~Applicable Systems~~”~~ identified in *CIP-011-4~~3~~ Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-4~~3~~ Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-4~~3~~ Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4~~3~~ Table R1 – Information Protection Program

Part	Applicable Systems	Requirements	Measures
1.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of ~~acceptable~~ evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity’s information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity’s information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity’s information protection program.

CIP-011-4~~3~~ Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or

CIP-011-4~~3~~ Table R1 – Information Protection Program

Part	Applicable Systems	Requirements	Measures
			• Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-4~~3~~ Table R2 –~~ BES Cyber Asset~~ Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4~~3~~ Table R2 –~~ BES Cyber Asset~~ Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4~~3~~ Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal

Part	Applicable Systems	Requirements	Measures
2.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action~~Methods to prevent the unauthorized retrieval of BCSI from ~~the Cyber Asset data storage media~~Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).	Examples of ~~acceptable~~ evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-4~~3~~ Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~2.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.~~	~~Examples of acceptable evidence may include, but are not limited to, the following:~~ ~~• Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or~~ ~~• Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.~~

B. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-011-4~~3~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~documented, but~~ did not~~,~~ implement one or more BCSI protection program(s). (Requirement R1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity ~~implemented one or more documented processes but~~ did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from ~~the BES Cyber~~	The Responsible Entity ~~implemented one or more documented processes but~~ did not include disposal ~~or media destruction~~ processes to prevent the unauthorized retrieval of BCSI from an Applicable System~~the BES Cyber Asset~~. (Part 2.~~2~~1)	The Responsible Entity ~~has not~~neither documented nor implemented any processes for applicable requirement parts in CIP-011-4~~3~~ Table R2~~3~~ – ~~BES Cyber Asset~~ Reuse and Disposal. (Requirement R2)

R #	Violation Severity Levels (CIP-011-4~~3~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		~~Asset~~an Applicable System. (Part 2.1)		

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-3:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable systems listed in Requirement R1 to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring applicable systems listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited

to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's supply chain cyber risk management plan(s) did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1. OR The Responsible Entitiy's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in Requirement R1.
R2.	The Responsible Entity did not implement one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity did not implement the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1, and did not implement the use of process(es) for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				procuring applicable systems as specified in Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in Requirement R2.
R3.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 16th calendar month since the previous review.	The Responsible Entity exceeded the 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 17th calendar month since the previous review.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 18th calendar month since the previous review.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan”
- CIP-013-3 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the second draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022~~June 30–August 13, 2021~~

Anticipated Actions	Date
Final Ballot~~45-day formal comment period with ballot~~	April 2022~~August 29–October 11, 2021~~
Board adoption~~Final Ballot~~	May 2022~~October 19–28, 2021~~
~~Board adoption~~	~~November 4, 2021~~

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled "Project 2016-02 Draft 3 Definitions"

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.~~ and their associated cyber systems.~~

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-3:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact ~~BES Cyber Systems~~ ~~(~~BCS~~)~~, their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). ~~identified independently supporting these BCS or their associated EACMS and PACS.~~ The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable systems listed in R1 to identify and assess cyber security risk(s) to the ~~Bulk Electric System (~~BES~~)~~ from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring applicable systems listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity ~~developed one or more documented~~ supply chain cyber security risk management plan(s) ~~which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do~~did not include one of the parts in ~~Requirement R1 Part~~ 1.2.1 through Part 1.2.6.	The Responsible Entity ~~developed one or more documented~~ supply chain cyber security risk management plan(s) did not include two or more of the parts in ~~which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Part 1.2, but the plans do not include two or more of the parts in Requirement R1~~ Part 1.2.1 through Part 1.2.6.	The Responsible Entity's ~~developed one or more documented~~ supply chain cyber security risk management plan(s) ~~, but the plan(s)~~ did not include the use of process(es) in planning for procurement of applicable systems ~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES~~ as specified in Part 1.1.~~,~~ ~~or~~OR ~~-~~The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2.~~the plan(s) did not include the use of process(es) for procuring~~	The Responsible Entity's ~~developed one or more documented~~ supply chain cyber security risk management plan(s)~~, but the plan(s)~~ did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as~~ applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified ~~plan(s) did not include the use of process(es) for procuring BES Cyber Systems, and their associated EACMS,~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~BES Cyber Systems, and their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2.~~	~~PACS, and SCI, as specified in Requirement R1~~ Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the RequirementR1.
R2.	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems, and~~	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems, and~~	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s), but~~ did not implement the use of process(es) ~~in planning for procurement of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es)~~ for procuring applicable systems~~BES Cyber~~	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s), but~~ did not implement the use of process(es) in planning for procurement ~~of BES Cyber Systems, and their associated EACMS, PACS, and SCI, to identify and assess cyber security risk(s) to the BES~~applicable systems as specified in ~~Requirement R1~~ Part 1.1, and did not implement the use of process(es) for

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	~~their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but~~ did not implement one of the parts in ~~Requirement R1~~ Part 1.2.1 through Part 1.2.6.	~~their associated EACMS, PACS, and SCI, as specified in Requirement R1 Part 1.2, but~~ did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~Systems, and their associated EACMS, PACS, and SCI,~~ as specified in Requirement R1 Part 1.2.	procuring ~~BES Cyber Systems, and their associated EACMS, PACS, and SCI,~~applicable systems as specified ~~in Requirement R1~~ Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the ~~r~~Requirement R2.
R3.	The Responsible Entity ~~reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than~~ exceeds 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the	The Responsible Entity ~~reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than~~exceeds ~~16~~ 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in~~ut~~	The Responsible Entity exceeds 15 calendar months by review~~e~~ing~~d~~ and obtain~~ed~~ing CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the~~but did so more than 17 calendar months but less than or equal to~~ 18th calendar month~~s~~ since the	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review ~~as specified in the Requirement~~.

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~but less than or equal to~~ 16th calendar months since the previous review~~ as specified in the Requirement~~.	~~less than or equal to~~ the 17th calendar months since the previous review~~ as specified in the Requirement~~.	previous review.~~ as specified in the Requirement.~~	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modification to CIP Standards Implementation Plan”
- CIP-013-3 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019~~TBD~~	Modified to address directive in FERC Order No. 850.	Revised
2~~3~~	11/05/2020~~TBD~~	Approved by the NERC Board of Trustees.~~Virtualization conforming changes.~~	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
45-day formal comment period with ballot	February 18 – April 4, 2022

Anticipated Actions	Date
Final Ballot	April 2022
Board adoption	May 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled “Project 2016-02 Draft 3 Definitions”

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3~~2~~**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-3~~2~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. **Effective Date:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan" ~~for Project 2019-03~~.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact ~~BES Cyber Systems~~BCS and their associated Electronic Access Control or Monitoring Systems (EACMS),~~ and~~ Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable ~~BES Cyber S~~systems ~~and their associated EACMS and PACS~~listed in Requirement R1 to identify and assess cyber security risk(s) to the ~~Bulk Electric System~~BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring ~~BES Cyber~~applicable ~~S~~systems ~~, and their associated EACMS and PACS,~~listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor~~ for use in the BES Cyber System and their associated EACMS and PACS~~; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the

scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's ~~developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the~~ supply chain cyber risk management plan(s) ~~do~~did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's ~~developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the~~ supply chain cyber security risk management plan(s) ~~do~~did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's ~~developed one or more documented supply chain cyber security risk management plan(s), but the~~supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~ applicable systems as specified in Part 1.1.~~,~~ OR The Responsible Entitiy's supply chain cyber security risk management ~~or the~~ plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and~~	The Responsible Entity's ~~developed one or more documented supply chain cyber security risk management plan(s), but the~~ supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement ~~of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~ applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~ applicable systems as specified in Part 1.2. OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~PACS,~~ applicable systems as specified in Part 1.2.	The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in ~~the~~ Requirement R1.
R2.	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but~~ did not implement one	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but~~ did not implement two	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or~~ did not implement the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~ applicable systems as	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s), but~~ did not implement the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~ applicable systems as specified in ~~Requirement R1~~ Part 1.1, and did not implement the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~ applicable systems as

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	of the parts in ~~Requirement R1~~ Part 1.2.1 through Part 1.2.6.	or more of the parts in ~~Requirement R1~~ Part 1.2.1 through Part 1.2.6.	specified in ~~Requirement R1~~ Part 1.2.	specified in ~~Requirement R1~~ Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in ~~the~~ ~~r~~Requirement R2.
R3.	The Responsible Entity exceeded 15 calendar months by reviewing~~ed~~ and obtaining~~ed~~ CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than15 calendar months but less than or equal to~~in the 16th calendar month~~s~~ since the previous review.~~ as specified in the Requirement~~	The Responsible Entity exceeded the 15 calendar months by reviewing~~ed~~ and obtaining~~ed~~ CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than but less than or equal to~~ in the 17th calendar month~~s~~ since the previous review~~ as specified in the Requirement~~.	The Responsible Entity exceeded 15 calendar months by reviewing~~ed~~ and obtaining~~ed~~ CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than 17 calendar months but less than or equal to~~in the 18th calendar month~~s~~ since the previous review~~ as specified in the Requirement~~.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review~~ as specified in the Requirement~~.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan” ~~for Project 2019-03~~
- CIP-013-3~~2~~ Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	

Project 2016-02 Modifications to CIP Standards Implementation Plan

Applicable Standard(s)

- Reliability Standard CIP-002-7 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-Y – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-8 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-8 – Cyber Security – BES Cyber System Logical Isolation
- Reliability Standard CIP-006-7 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-7 – Cyber Security – System Security Management
- Reliability Standard CIP-008-7 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-5 – Cyber Security – Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-4 – Cyber Security – Information Protection
- Reliability Standard CIP-013-3 – Cyber Security – Supply Chain Risk Management
- Proposed new or modified terms listed in the "CIP Definitions Posting Document (Project 2016-02)"

These standards and Definitions of Terms used in the versions listed above of the CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

These standards and new and modified terms used in the standards above will be referenced as the "Revised CIP Standards and Definitions" within the Implementation Plan.

Requested Retirement(s)

- Reliability Standard CIP-002-6 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-Y – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-7 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)
- Reliability Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-6 – Cyber Security – System Security Management

- Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-3 – Cyber Security – Information Protection
- Reliability Standard CIP-013-2 – Cyber Security – Supply Chain Risk Management
- Proposed terms for retirement listed in the “Definitions of Terms used in the above listed CIP Cyber Security Standards” document

These standards and definitions used in the versions listed above will be referenced as the “Requested CIP Retired Standards and Definitions” within the Implementation Plan.

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved or retired before the Applicable Standard become effective:

- BES Cyber Asset (BCA)
- BES Cyber System Information (BCSI)
- CIP Senior Manager
- Cyber Assets
- Cyber Security Incident
- Cyber System
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate Systems (IS)
- Management Interface
- Physical Access Control Systems (PACS)
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Removable Media

- Reportable Cyber Security Incident
- Shared Cyber Infrastructure (SCI)
- Transient Cyber Asset (TCA)
- Virtual Cyber Asset (VCA)

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions. The intent of the Compliance Dates for Early Adoption of Revised CIP Standards and Definitions section is to permit Responsible Entities the adoption to comply with the Revised CIP Standards and Definitions prior to the Effective Date.

Effective Date and Phased-in Compliance Dates

The Effective Dates for the Revised CIP Standards and Definitions are provided below. As noted in the General Considerations section above, the standard drafting team determined to clarify initial performance of periodic requirements and permit Responsible Entities to comply with the Revised CIP Standards and Definitions prior to the effective date. These provisions are also provided below.

Revised CIP Standards and Definitions

Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

---

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Where approval by an applicable governmental authority is not required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the date the Revised CIP Standards and Definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards and Definitions.

Compliance Dates for Early Adoption of Revised CIP Standards and Definitions

A Responsible Entity may elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the Revised CIP Standards and Definitions. Responsible Entities must comply with applicable Requested CIP Retired Standards and Definitions until that date.

Planned or Unplanned Changes

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-7, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-7, Attachment 1, criteria.

For unplanned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirement not applicable to Medium impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Retirement Date

Requested CIP Retired Standards and Definitions

The Requested CIP Retired Standards and Definitions shall be retired immediately prior to the effective date of the Revised CIP Standards and Definitions in the particular jurisdiction in which the Revised CIP Standards and Definitions are becoming effective.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2016-02 ~~Virtualization~~Modifications to CIP Standards Implementation Plan

Applicable Standard(s)

- Reliability Standard CIP-002-7 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-Y~~9~~ – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-8~~7~~ – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-8 – Cyber Security – BES Cyber System Logical Isolation
- Reliability Standard CIP-006-7 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-7 – Cyber Security – System Security Management
- Reliability Standard CIP-008-7 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-5 – Cyber Security – Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-4~~3~~ – Cyber Security – Information Protection
- Reliability Standard CIP-013-3 – Cyber Security – Supply Chain Risk Management
- Proposed new or modified terms listed in the “CIP Definitions Posting Document (Project 2016-02)”

  These standards and Definitions of Terms used in the versions listed above of the CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

  These standards and new and modified terms used in the standards above will be referenced as the “Revised CIP Standards and Definitions” within the Implementation Plan.

Requested Retirement(s)

- Reliability Standard CIP-002-6 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-Y~~8~~ – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-7~~6~~ – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)
- Reliability Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-6 – Cyber Security – System Security Management

- Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-3~~2~~ – Cyber Security – Information Protection
- Reliability Standard CIP-013-2 – Cyber Security – Supply Chain Risk Management
- Proposed terms for retirement listed in the “Definitions of Terms used in the above listed CIP Cyber Security Standards” document

These standards and definitions used in the versions listed above will be referenced as the “Requested CIP Retired Standards and Definitions” within the Implementation Plan.

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved or retired before the Applicable Standard become effective:

- BES Cyber Asset (BCA)
- ~~BES Cyber System~~
- BES Cyber System Information (BCSI)
- CIP Senior Manager
- Cyber Assets
- Cyber Security Incident
- Cyber System
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate Systems (IS)
- Management Interface
- ~~Management Module~~
- ~~Management Systems~~
- Physical Access Control Systems (PACS)
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Removable Media
- Reportable Cyber Security Incident
- ~~Self-Contained Application~~
- Shared Cyber Infrastructure (SCI)
- Transient Cyber Asset (TCA)

- Virtual Cyber Asset (VCA)

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions. The intent of the Compliance Dates for Early Adoption of Revised CIP Standards and Definitions section is to permit Responsible Entities the adoption to comply with the Revised CIP Standards and Definitions prior to the Effective Date.

Effective Date and Phased-in Compliance Dates

The Effective Dates for the Revised CIP Standards and Definitions are provided below. As noted in the General Considerations section above, the standard drafting team determined to clarify initial performance of periodic requirements and permit Responsible Entities to comply with the Revised CIP Standards and Definitions prior to the effective date. These provisions ~~also~~ are also provided below.

Revised CIP Standards and Definitions

Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the date the Revised CIP Standards and Definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

---

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards and Definitions.

Compliance Dates for Early Adoption of Revised CIP Standards and Definitions

A Responsible Entity may elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the Revised CIP Standards and Definitions. Responsible Entities must comply with applicable Requested CIP Retired Standards and Definitions until that date.

Planned or Unplanned Changes

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7~~6~~, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7~~6~~, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-~~6~~7, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-~~6~~7, Attachment 1, criteria.

For unplanned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirement not applicable to Medium impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Retirement Date

Requested CIP Retired Standards and Definitions

The Requested CIP Retired Standards and Definitions shall be retired immediately prior to the effective date of the Revised CIP Standards and Definitions in the particular jurisdiction in which the Revised CIP Standards and Definitions are becoming effective.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards
Draft 3

The standard drafting team (SDT) is seeking comment on the following new, modified, or retired terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the ~~r~~Reliable ~~o~~Operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS)	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	Acronym only.
BES Cyber System Information	Information about the BES Cyber System that could be used to gain	Information about the BES Cyber System or Shared Cyber

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
(BCSI)	unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	Infrastructure that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC ~~CIP Standards, CIP-002 through CIP-011~~Critical Infrastructure Protection Standards.
Cyber Assets	Programmable electronic devices, including the hardware, software, and	Programmable electronic devices, including the hardware, software,

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
	data in those devices.	and data in those devices; excluding Shared Cyber Infrastructure.
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: • For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, ~~or~~ (3) an Electronic Access Control or Monitoring System; or (4) Shared Cyber Infrastructure; or • Disrupts or attempts to disrupt the operation of a BES Cyber System.
Cyber System ***New Definition***		A group of one or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Intermediate Systems.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	An electronic policy enforcement point or a Cyber Asset interface that ~~on an Electronic Security Perimeter that allows~~controls routable communication to and from a BES Cyber System ~~between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter~~.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System ~~from a Cyber Asset that is outside of its associated~~through its ~~Electronic Security Perimeter~~ ESP via a bi-directional routable protocol connection.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more EAPs.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated access by a person using a Cyber Asset or VCA, not protected by any of the ~~employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the~~ Responsible Entity's Electronic Security Perimeter(s) (ESP) and using a routable protocol: • To a Cyber System protected by an ESP; • That is converted to a non-routable protocol to a Cyber System not protected by an ESP; or • To a Management Interface of Shared Cyber Infrastructure.
Intermediate System~~s~~	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users. ~~A Cyber Asset or collection of Cyber Assets performing access control to~~

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
		~~restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.~~
Management Interface ***New Definition***		An administrative interface of a~~n~~ ~~SCI~~Shared Cyber Infrastructure or Electronic Access Control or Monitoring System that: • Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or • Is an autonomous subsystem that provides access to power management or the physical console independently of the host system's CPU, firmware, and operating system; or • Configures an Electronic Security Perimeter.~~;~~ Physical user interfaces are excluded (e.g., power switch, touch panel, etc.).
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers	Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
	reside, and for which access is controlled.	Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	One or more Cyber Assets or Virtual Cyber Assets that: • ~~connected using a routable protocol~~Are ~~within~~ protected by ~~or on~~ an Electronic Security Perimeter (ESP) but are ~~that is~~ not part of the highest impact BES Cyber System ~~within~~ protected by the same ~~Electronic Security Perimeter~~ESP; or • ~~.~~Share CPU or memory with any part of the ~~The impact rating of Protected Cyber Assets is equal to the highest rated~~ BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to ~~in the~~ an ~~same~~ ESP.
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, Shared Cyber Infrastructure, a network ~~within~~ protected by an ESP, or a Protected Cyber Asset. ~~Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives~~

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
		~~that contain nonvolatile memory.~~
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; ~~or~~ - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or - Shared Cyber Infrastructure supporting a BES Cyber System
Shared Cyber Infrastructure (SCI) ***New Definition***		One or more programmable electronic devices, including the software that shares the devices' resources, that: - In a clustered configuration, hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or - Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
		associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization. SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer,	A Cyber Asset or Virtual Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. ~~directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication)~~connected for 30 consecutive calendar days or less ~~to a~~: ~~• BES Cyber Asset,~~ • To a network ~~within~~ protected by an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	vulnerability assessment, maintenance, or troubleshooting purposes.	communication) to a: • BES Cyber Asset, or • Shared Cyber Infrastructure, or • PCA associated with high or medium impact BES Cyber Systems. Virtual machines hosted on a physical TCA are treated as software on that physical TCA. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Virtual Cyber Asset (VCA) ***New Definition***		A non-dormant logical instance of an operating system or firmware, on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure; excluding logical instances that are being actively remediated.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Virtualization - Draft 3

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on the **CIP Virtualization suite of Standards** by **8 p.m. Eastern, Monday, April 4, 2022.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Jordan Mallory (via email) or at 404-446-2589.

Background Information

Project 2016-02 (1) addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and (2) considers the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for Standard Drafting Team Consideration (V5TAG Transfer Document).

The V5TAG, which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP Version 5 standards and to support industry's implementation activities. During the V5TAG's activities, it identified certain issues with the CIP Reliability Standards that would be better addressed by a standard drafting team (SDT) for the CIP Reliability Standards. The V5TAG developed the CIP Version 5 Transition Advisory Group Issues for Consideration document to formally recommend that the SDT address these issues and consider modifications to the standard language during the standards development process. Among other issues, the V5TAG stated "The CIP Version 5 standards comments.

Summary of Changes Overview

The SDT reviewed all comments and made modifications to the Reliability Standards and Definitions accordingly. Below are questions for which the SDT is seeking industry input. In order to allow the SDT to sort comments received by topic, the SDT respectfully requests comments be submitted with the respective question topic. The SDT thanks all stakeholders for your time and responses during this comment period.

Questions

1. The SDT has redefined Shared Cyber Infrastructure (SCI) such that it now focuses on cyber infrastructure that shares its hardware resources among VCAs of different impact levels only, which then subjects the SCI to additional requirements. Virtualization infrastructure that only hosts VCAs or associated VCAs of the same impact level is no longer SCI and requires no recategorization from current state. The SDT also removed the SCI identification changes from CIP-002. The SDT believes this greatly simplifies SCI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

2. The SDT has reinstated the currently approved ESP definition and appended language to allow for zero trust models. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal. Please also include any comments on the proposed EAP definition in the response to this question.

   ☐ Yes
   ☐ No

   Comments:

3. The SDT modified the ERC definition from the “outside the asset containing” reference point in the previous draft back to an ESP reference point. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

4. The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

5. The SDT modified the VCA definition primarily to include the ability to host them on numerous asset types other than SCI. This allows for current state, where entities consider hypervisors as BCA, EACMS, etc. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

6. The SDT modified numerous other glossary terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

7. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

8. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

9. The SDT revised CIP-010 R1 to focus on defining change, authorizing change, and verifying that CIP-005 and CIP-007 related security controls are not affected by changes. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

10. The SDT made other revisions to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

    ☐ Yes
    ☐ No

    Comments:

11. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

    ☐ Yes
    ☐ No

    Comments:

12. The SDT has revised numerous VSL's for simplification. Do you agree with the proposed changes? If not, please provide the basis for your disagreement.

    ☐ Yes
    ☐ No

    Comments:

13. The SDT has revised the Implementation Plan to include the Planned and Unplanned Changes provisions and to allow for early adoption. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

    ☐ Yes
    ☐ No

    Comments:

14. Please provide any additional comments for the drafting team to consider, if desired.

Technical Rationale

Project 2016-02 Modifications to CIP Standards
New and Modified Terms, and Exemption Language Used in NERC Reliability Standards

Proposed Modified Terms

BES Cyber Asset (BCA)

A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Rationale

The BCA definition is changing to allow for BCA to be either Cyber Assets (hardware included) or Virtual Cyber Assets (VCA) (software only virtual machines without the underlying hardware). See the VCA and Shared Cyber Infrastructure (SCI) definition below.

BES Cyber System Information (BCSI)

Information about the BES Cyber System or Shared Cyber Infrastructure that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

Rationale

Conforming changes such that BCSI includes information about SCI.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Standards.

Rationale

Remove explicit reference to the CIP standards as only "CIP-002 through CIP-011" as the body of CIP standards has grown beyond CIP-011. As an example, the CIP Senior Manager also has requirements within CIP-013.

Cyber Assets

Programmable electronic devices, including the hardware, software, and data in those devices; excluding Shared Cyber Infrastructure.

Rationale

Modified to explicitly exclude SCI from the definition of Cyber Asset such that SCI is a different hardware class on which the other VCAs of differing impact levels execute. SCI is defined separately such that it can be the object of additional requirements based on its unique risks.

Cyber Security Incident

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System, or (4) Shared Cyber Infrastructure; or
- Disrupts or attempts to disrupt the operation of a BES Cyber System.

Rationale

Modified to add SCI to the scope of compromised or attempted compromise systems.

Electronic Access Control or Monitoring Systems (EACMS)

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or Shared Cyber Infrastructure. This includes Intermediate Systems.

Rationale

Modified to add VCA and SCI as two other forms that an EACMS can take and add SCI as an object of the access control or monitoring.

Electronic Access Point (EAP)

An electronic policy enforcement point or a Cyber Asset interface that controls routable communication to and from a BES Cyber System.

Rationale

As network security moves deeper into the infrastructure, it's no longer necessary to prescribe that network security be performed only at a 'Cyber Asset interface on an ESP'; at one point on a network edge. Zero Trust, for example, highly distributes the network security model and is not perimeter-based, and this is incorporated through the addition of "electronic policy enforcement point or". With the added flexibility in CIP-005 to adopt these models in addition to the traditional Electronic Security Perimeter (ESP) model, the term EAP is being modified to allow for electronic policy enforcement points and no longer prescribes an architecture.

External Routable Connectivity (ERC)

The ability to access a BES Cyber System through its ESP via a bi-directional routable protocol connection.

Rationale

The ERC definition is changing to allow for zero trust or other network models that are not strictly perimeter or network-border based, thus not having concepts of "inside" or "outside". These concepts are replaced with the language "through its ESP" so that it does not imply a prescriptive network security model. The ERC term is used throughout the CIP Standards within the Applicable Systems column as a scoping mechanism based on the inherent risk associated with external routable connectivity as well as to limit the scope of requirements that would require ERC to function. The SDT is maintaining this use of ERC, but also clarifying the relationship between ERC and IRA in that a non-routable, serial only BCS may have ERC and have IRA through the ERC through a subsequent IP/serial conversion (see changes to IRA definition).

Electronic Security Perimeter (ESP)

A logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more EAPs.

Rationale

The traditional network border ESP remains a valid network security model, however it is no longer the only prescribed model as CIP-005 allows other access control models that are not based on network perimeters such as Zero Trust architectures. The proposed ESP definition retains its current definition but appends "or a logical boundary defined by one or more EAPs" to incorporate models that move away from implicit trust within network perimeters and using network location as a primary factor in access control decisions. In these models, the perimeter shrinks to increasingly more granular levels, potentially down to a process or resource level on a BCS. The proposed definition allows for an ESP to be (a) static point(s) on a network boundary such as a traditional firewall as an EAP that is enforcing access policies or configurations (e.g., firewall rulesets), (b) many dynamic, short-lived, session-level 'perimeters' established at time of access that are network independent (e.g., users to resources, for example), or (c) hybrid implementations combining elements of both.

The SDT has kept the 'logical border' concept for the "surrounding a network" ESP and used the language "logical boundary" for zero trust models. A 'border' does indeed surround an object, in this case a network, but a 'boundary' may not surround or enclose, it's a line that can be crossed, such as a policy enforcement point controlling access to a resource. The SDT has also updated language in the standards to remove concepts such as 'inside' an ESP and replaced that with more inclusive phrases such as 'protected by' an ESP.

Interactive Remote Access (IRA)

User-initiated access by a person using a Cyber Asset or VCA, not protected by any of the Responsible Entity's Electronic Security Perimeters (ESP), and using a routable protocol:

- to a Cyber System protected by an ESP;
- that is converted to a non-routable protocol, to a Cyber System not protected by an Electronic Security Perimeter; or
- To a Management Interface of Shared Cyber Infrastructure

Rationale

The proposed IRA definition changes in two fundamental ways: (1) to incorporate as IRA situations where a BCS has ERC and through it users outside of any of the Responsible Entity's ESPs have access to non-routable (serial) Cyber Systems within the asset through a subsequent IP/serial conversion, and (b) to include the Management Interfaces of SCI as targets of IRA. The references to ownership of the remote client have been removed.

Intermediate Systems

One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.

Rationale

The IS definition is changing to remove requirement language (i.e., where an Intermediate System must reside) embedded within the definition. That language has been moved to CIP-005 R2 within a mandatory requirement. The definition was also updated from a Cyber Asset focus to an EACMS focus to include more forms (i.e., VCA) the Intermediate System can take.

Physical Access Control Systems (PACS)

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Rationale

Modified to add VCA and SCI as two other forms that a PACS can take.

Physical Security Perimeter (PSP)

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Rationale

The PSP definition is changing to add SCI as type of device to be included within a PSP.

Protected Cyber Asset (PCA)

One or more Cyber Assets or Virtual Cyber Assets that:

- Are within an Electronic Security Perimeter but are not part of the highest impact BES Cyber System within the same Electronic Security Perimeter; or
- Share CPU or memory with any part of a BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to the ESP.

Rationale

The PCA definition is being updated to include "share CPU or memory with any part of a BES Cyber System" to mitigate the risks of hardware-based vulnerabilities (Spectre, Meltdown, Rowhammer, etc.) on Shared Cyber Infrastructure for any virtual machines allowed to run on the same hardware as BES Cyber Systems. Since virtualization can allow systems of differing trust levels to simultaneously execute on the same hypervisor servers in the hardware underlay and thus share the same CPU and memory, this addition to the PCA definition requires that those VCAs that do share CPU and memory with a BCS become associated PCA's of the BCS. This provides the high water marking of VCAs sharing a single hypervisor's CPU or memory. Affinity rules can be used within the virtualization configuration to prevent this situation and keep other VCAs from becoming associated PCAs. Finally, the definition is being modified to account for "remediation VLAN" automation of security controls where a VCA may instantiate in a logical network reserved for vulnerability assessment and updates (OS patches, AV updates, etc.). The intent is the VCA does not become a PCA while temporarily in this state as its being updated prior to being connected to its production network.

Removable Media

Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, Shared Cyber Infrastructure, a network protected by an ESP, or a Protected Cyber Asset.

Rationale

The Removable Media definition is being updated to add SCI as a target of the Removable Media connection and incorporate the new ESP definition.

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BES Cyber System;
- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or
- Shared Cyber Infrastructure supporting a BES Cyber System.

Rationale

This definition is being modified to add compromised or disrupted SCI supporting a BCS as a target.

Transient Cyber Asset (TCA)

A Cyber Asset or Virtual Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. connected for 30 consecutive calendar days or less:
   a. to a network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or
   b. directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a:
      i. BES Cyber Asset,
      ii. Shared Cyber Infrastructure, or
      iii. Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Virtual machines hosted on a physical TCA are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Rationale

The TCA definition is being updated to add VCA as a form a TCA can take. The intent is to handle VCAs that are created for typical TCA uses but are normally dormant (e.g. a VCA with Wireshark for troubleshooting network issues within a virtualized infrastructure). Additionally, SCI was added as a target to which TCA's can be directly connected. The statement "Virtual machines hosted on a physical TCA are treated as software on that physical TCA" is to clarify that on a physical TCA (laptop) with hypervisor software and one or more VCA images, the hypervisor and VCAs are treated as software on the one physical TCA. This is to clarify that the one physical TCA does not have to be tracked as multiple distinct virtual TCAs. Corresponding clarifications have been made to the methods in CIP-003 and CIP-010 used to mitigate the risks of TCA software.

Proposed New Terms

Cyber System

A group of one or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.

Rationale

This proposed new term is used to simplify applicability when referring in the standards or other definitions to all the forms an object may take (CA, VCA, or SCI). If other forms are needed in the future, their addition to this one definition can reduce needed edits throughout the standards.

Management Interface

An administrative interface of an SCI or EACMS that:

- Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or
- Is an autonomous subsystem that provides access to power management or the physical console independently of the host system's CPU, firmware, and operating system; or
- Configures an Electronic Security Perimeter;

excluding physical user interfaces (e.g., power switch, touch panel, etc.).

Rationale

This term is being defined so that requirements can be addressed to SCI and EACMS Management Interfaces to target the unique risks for virtualized environments presented by the management 'consoles' for such environments. With 'infrastructure as a service' (IaaS) environments, the management consoles can not only be used to create, but also to destroy or reconfigure virtual servers, networks, switches, firewalls, etc. The term also includes interfaces commonly known as ILO (Integrated Lights Out), that can be used to remotely manage hardware (usually including power on/off, access to the physical console, etc.). It also includes interfaces used to configure an ESP (such as on firewalls or a network switch that is enforcing an ESP between different logical networks (e.g., VLANs).

Shared Cyber Infrastructure (SCI)

One or more programmable electronic devices, including the software that shares the devices' resources, that:

- In a clustered configuration, hosts one or more Virtual Cyber Assets (VCA) included in a BCS or their associated EACMS or PACS; and also hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or
- Provides storage resources required for system functionality of one or more CAs or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more CAs or VCAs that are not included in, or associated with, BCS of the same impact categorization.

SCI does not include the supported VCA or Cyber Assets with which it shares its resources.

Rationale

The SCI definition is being created to separate the underlying hardware from VCAs in the situation where the shared hardware resources support VCAs of varying impact levels. This allows security requirements to be targeted to SCI to address the unique risks of shared hardware. There are many requirements that now include the newly defined term SCI in the "Applicable Systems" column to maintain security level parity with traditional Cyber Assets.

Beyond security level parity with protecting a typical hardware based Cyber Asset, the SCI can have a more significant impact in a virtualized environment since it can host, and therefore impact, multiple virtualized systems of varying impact levels. Because of this capability, some additional controls only apply to SCI, such as the management plane isolation required by the proposed CIP-005. Addressing these unique risks requires separation of the hardware underlay into a separate definition.

The phrase "SCI does not include the supported VCA or Cyber Assets with which it shares its resources" is included to clarify that, for example, electronic access to a hosted VCA by a user is not electronic access to the SCI on which it executes.

Of note is that shared network devices are not in the scope of this definition. Since network switches and firewalls share their resources by nature, this exclusion avoids pulling all network hardware into scope as SCI. However, network switches and other hardware that does enforce an ESP (such as a network switch configured to logical isolate different VLANs) comes into scope as an EACMS.

Virtual Cyber Asset (VCA)

A non-dormant logical instance of an operating system or firmware, on a virtual machine hosted on a BCA, EACMS, PACS, PCA, or SCI, excluding logical instances that are being actively remediated.

Rationale

The NERC Glossary definition of Cyber Asset has a direct tie to the hardware on which it relied. This affected the definitions of the "Applicable Systems" terms such as BES Cyber Systems (BCS), EACMS, PACS, and Protected Cyber Assets (PCAs). Because the Reliability Standard is applicable to the aforementioned systems, the control for the Cyber Assets also applies to the hardware. This one-to-one relationship between a Cyber Asset and its underlying hardware is what virtualization intentionally breaks to increase reliability and resiliency by allowing Virtual Cyber Assets to be abstracted from the hardware and therefore able move to any available hardware out of a pool of resources. The proposed NERC Glossary definition of Virtual Cyber Asset (VCA) allows the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined.

The phrase "non-dormant logical instance" is used to clarify that a VCA does not include disk image files that are not currently instantiated or executing and thus providing no functions or services. Likewise, the phrase "excluding logical instances that are being actively remediated" excludes those that are instantiated but are being remediated in an isolated environment before they are moved to production networks and begin providing their function or service.

The phrase "on a virtual machine" is used to clarify that a dedicated, non-virtualized Cyber Asset may have a 'logical instance of an Operating System (OS) or firmware', but that is not a VCA. Such a logical instance of an OS or firewall on a virtual machine is a VCA.

The phrase "hosted on a BCA, EACMS, PACS, PCA, or SCI" is to clarify that an entity for an "all-in" scenario can still classify the underlying hardware as one or several of these types, yet the VCA's remain their own object subject to requirements and are not simply "software in the device" as in the Cyber Asset definition.

Examples of Virtual Cyber Assets may include, but are not limited to, logical instances of the following:

- Operating Systems (Virtual Machines (VM));
- Networking devices such as switches, routers, and load balancers;
- Security appliances such as firewalls and VPN concentrators; and
- Helper appliances with logical connectivity (such as malware detection, plugins, etc.).

Proposed Retired Terms

None

Technical Rationale for Exemptions Section

Rationale for Exemption 4.2.3.1

The term 'Cyber Assets' was changed to the new proposed term 'Cyber Systems'. Rather than changing this language to a list of all possible forms (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure) as the object of the exemption, the SDT chose to instead use the existing language in the 4.2.3.4 and 4.2.3.5 exemptions such that all five exemptions use a form of 'systems' as their object.

Rationale for Exemption 4.2.3.2 and 4.2.3.3

In 4.2.3.2, the term 'Cyber Assets' was changed to 'Cyber Systems' which is a new proposed glossary addition. Rather than changing these two exemptions to list all possible forms (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure), the SDT chose to define a new term that incorporates all forms and use it within the multiple exemptions and at other points within the standards.

For 4.2.3.3, the ability to move workloads or VM's seamlessly across different sites for increased resiliency can require different sites to be connected as a flat network without layer 3 ESP's at each discrete site (e.g., a layer 2 adjacency across the sites). A "Super ESP" as it's been historically known is created across the sites and thus an exemption based on having a discrete layer 3 ESP at each site no longer works to exclude, for example, the network transport equipment that may belong to carriers. The SDT is including the 4.2.3.3 exemption to further clarify this scenario. Responsible Entities should notice the exemption uses the word "between" – when extending an ESP between geographic locations, CIP-005 requires the confidentiality and integrity protection of the data (typically through encryption) between the relevant PSPs. This exemption then covers the related Cyber Systems "between" those encryption points but does not exclude the endpoints performing the encryption.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — BES Cyber System Categorization

Technical Rationale and Justification for Reliability Standard CIP-002-7

February 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-002-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-002-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-002-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a SDT. The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Attachment 1 – Impact Rating Criteria

Change Rationale:

In the medium impact rating criterion 2.1 referencing shared BCS for commissioned generation, the SDT has proposed a change to incorporate an earlier approved Request For Interpretation (RFI). The RFI was submitted seeking clarification of Criterion 2.1 of Attachment 1 regarding the use of the phrase "shared BES Cyber Systems." The resulting approved interpretation was introduced as Appendix 1 in CIP-002-5.1a.

The SDT incorporated the interpretation into CIP-002-7 Attachement 1 criterion 2.1 by modifying it to reference "each discrete shared BCS" and removed the RFI appendix from the standard.

Former Background Section from Reliability Standard CIP-002-5.1a

The **Background** section has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

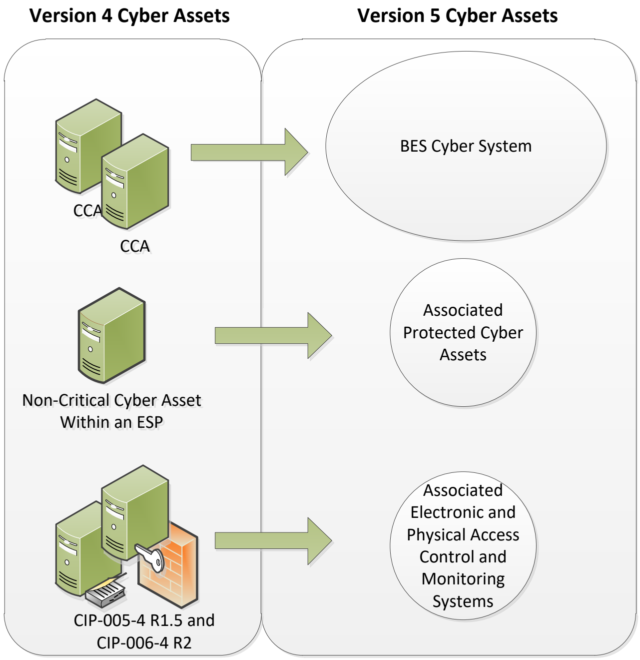
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS")

Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")

Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA")

Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

Technical Rationale for Reliability Standard CIP-002-5.1a

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from the CIP-002-5.1a standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1a

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints

- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
    - Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)

        - Special Protection Systems or Remedial Action Schemes
    - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
        - Under and Over Frequency relay protection (includes automatic load shedding)
    - Sensors, relays & breakers (DP)
        - Under and Over Voltage relay protection (includes automatic load shedding)
    - Sensors, relays & breakers (DP)
        - Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
    - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
    - Software used to perform calculation (BA)
- Demand Response
    - Ability to identify load change need (BA)
    - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
    - Ability to identify load change need (BA)
    - Ability to implement load changes (TOP, DP)
- Non-spinning reserve (contingency reserve)
    - Know generation status, capability, ramp rate, start time (GO, BA)
    - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
    - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
    - Software to calculate unit adjustments (BA)
    - Transmit adjustments to individual units (GOP)
    - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
    - Frequency source, schedule (BA)
    - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
    - Sensors, stator control system, feedback (GO)
- Capacitive resources
    - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
    - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
    - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
    - SCADA (TOP, GOP)
    - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
    - Through black start units (TOP, GOP)
    - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term “Facilities”, there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports

the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.

- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1’s medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is “to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance.” In particular, it requires that “as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency.” The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

  The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities’ qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a “long term” reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as “Reliability Must Run,” and this designation is distinct from those generation Facilities designated as “must run” for market stabilization purposes. Because the use of the term “must run” creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.
- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.
- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.
- Criterion 2.13 categorizes as medium impact those BA Control Centers that “control” 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.
- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:
    - Excluded radial facilities that would only provide support for single generation facilities.
    - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

- 230 kV –> 700 MVA
- 345 kV –> 1,300 MVA
- 500 kV –> 2,000 MVA
- 765 kV –> 3,000 MVA

In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

- For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.
- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

  - Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.
- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.
- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.
- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

  In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

  The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

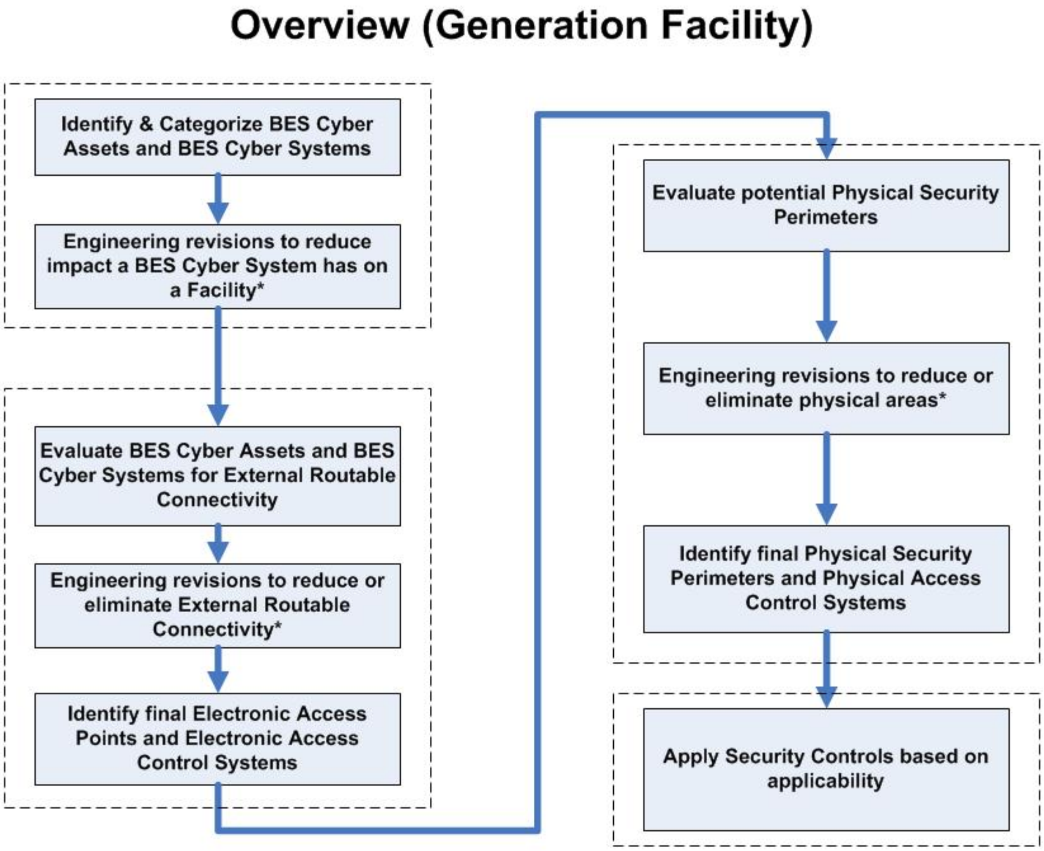
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.


Overview (Generation Facility)

* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of “bright-line” criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager’s approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Appendix 1

Requirement Number and Text of Requirement

CIP-002-5.1, Requirement R1

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

i. Control Centers and backup Control Centers;

ii. Transmission stations and substations;

iii. Generation resources;

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;

v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and

vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

Attachment 1, Criterion 2.1

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

1.1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions

Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase “shared BES Cyber Systems.”

The Interpretation Drafting Team identified the following questions in the RFI:

1. Whether the phrase “shared BES Cyber Systems” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?
2. Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

Responses

Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)

Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:

> The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-Y

February 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-003-Y

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-9. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-Y is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document stated, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to shorten applicability statements within the body of CIP standards with "BCS" as the defined acronym for "BES Cyber System".

Requirement R2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to align security management control requirements with the virtualization changes.

To ensure SCI supporting low impact BCS is afforded equal security controls as the BCS, the SDT added "SCI that supports any part of a low impact BCS".

Attachment 1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to shorten applicability statements within the body of CIP standards with “BCS” as the defined acronym for “BES Cyber System”.

To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a system(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term system(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Attachment 1 Section 2

Rationale

To ensure virtual infrastructure providing electronic access controls for the low impact BCS is afforded equal physical security controls as the physical Cyber Assets that provide electronic access controls for the low impact BCS, the SDT modified this section to include the Virtual Cyber Asset (VCA) where only Cyber Assets had previously been listed.

Attachment 1 Section 3

Attachment 1 Section 3 Part 3.1

Rationale

Part 3.1(i)

To ensure an asset containing a low impact BCS or an SCI supporting a low impact BCS is afforded equal electronic access controls as the low impact BCS, the SDT added “SCI that supports any part of a low impact BCS”.

To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a Cyber System(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term Cyber System(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Part 3.1(ii) To ensure only necessary inbound and outbound electronic access is permitted for SCI supporting a low impact BCS just as is required for access control to the low impact BCS, the SDT adjusted the language to include communications that are between SCI that supports any part of a low impact BCS and a system(s) outside the asset(s) containing the SCI that supports any part of a low impact BCS.

Attachment 1 Section 3 Part 3.2

Rationale

To ensure SCI supporting low impact BCS are afforded equal electronic access controls for Dial-up Connectivity, the SDT added “the asset containing the SCI that supports any part of a low impact BCS” to the low impact BCS. Per VCA capability was included in addition to per Cyber Asset capability to accommodate for incapability of both physical and virtual aspects of the low impact BCS or its associated SCI.

Attachment 1 Section 5

Rationale

To ensure SCI supporting a low impact BCS are afforded equal mitigations from the introduction of malicious code as the low impact BCS, the SDT added “SCI that supports any part of a low impact BCS” to the low impact BCS.

Attachment 1 Section 5 Part 5.1

Rationale

To enable for virtualization technologies and capabilities the SDT added, “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code” as an option in Attachment 1 Section 5 Part 5.1.

Attachment 1 Section 5 Part 5.2

Rationale

To ensure SCI supporting a low impact BCS are afforded equal protections when a TCA managed by a party other than the Responsible Entity is used, the SDT added “SCI that supports any part of a low impact BCS” to the low impact BCS in Attachment 1 Section 5 Part 5.2.1.

To enable for virtualization technologies and capabilities the SDT added, “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code” as an option in Attachment 1 Section 5 Part 5.2.1.

The final bullet of Attachment 1 Section 5 Part 5.2.1 was preceded with the language “Review of” to make the requirement for other methods parallel to the five options listed above it.

Attachment 1 Section 5 Part 5.3

Rationale

To ensure SCI supporting a low impact BCS are afforded equal protections from malicious code when using Removable Media, the SDT added “SCI that supports any part of a low impact BCS” to the low impact BCS in Attachment 1 Section 5 Parts 5.3.1 & 5.3.2.

Part 3.1 (iii) The SDT replaced the undefined ‘intelligent electronic devices’ with the defined term ‘Protection Systems’.

Attachment 1 Section 3 Part 3.2

Rationale

To ensure SCI supporting low impact BCS are afforded equal electronic access controls for Dial-up Connectivity, the SDT added “SCI that supports any part of a low impact BCS”. To incorporate other forms, the ‘per Cyber Asset capability’ was changed to ‘per system capability’.

Attachment 1 Section 5

Attachment 1 Section 5 Part 5.1

Rationale

To enable for virtualization technologies and capabilities the SDT added, “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code” as an option in Attachment 1 Section 5 Part 5.1.

Attachment 1 Section 5 Part 5.2

Rationale

To enable for virtualization technologies and capabilities the SDT added, “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code” as an option in Attachment 1 Section 5 Part 5.2.1.

The final bullet of Attachment 1 Section 5 Part 5.2.1 was preceded with the language “Review of” to make the requirement for other methods parallel to the five options listed above it.

Attachment 1 Section 5 Part 5.3

Rationale

To ensure SCI supporting a low impact BCS are afforded equal protections from malicious code when using Removable Media, the SDT added “SCI that supports any part of a low impact BCS” to the low impact BCS in Attachment 1 Section 5 Parts 5.3.1 & 5.3.2.

Attachment 2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to shorten applicability statements within the body of CIP standards with “BCS” as the defined acronym for “BES Cyber System”.

Former Background Section from Reliability Standard CIP-003-8

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Technical Rational for Reliability Standard CIP-003-8

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-003-8 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access

For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only “necessary” inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for “necessary” inbound and outbound electronic access controls may be documented within the Responsible Entity’s cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

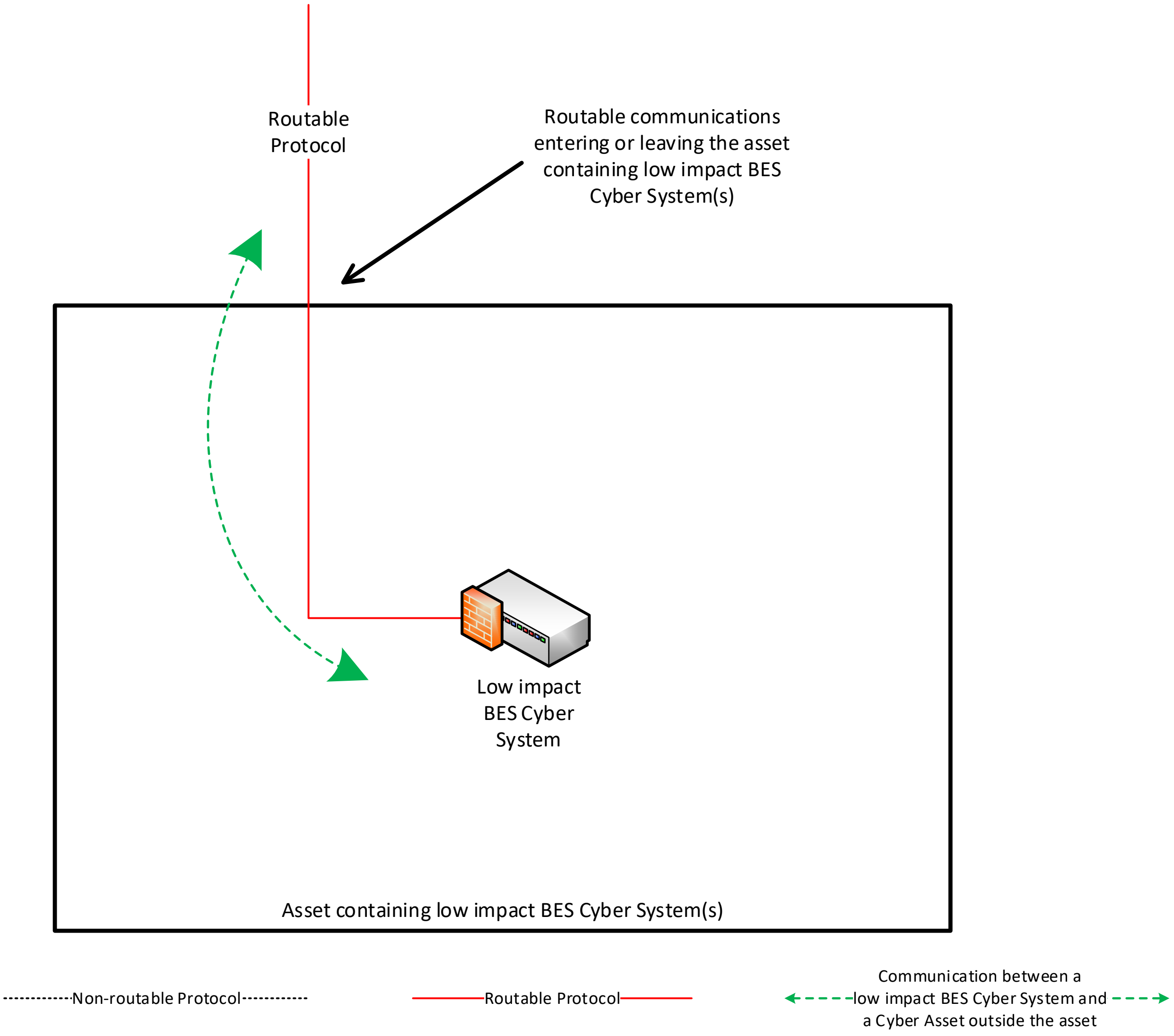
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

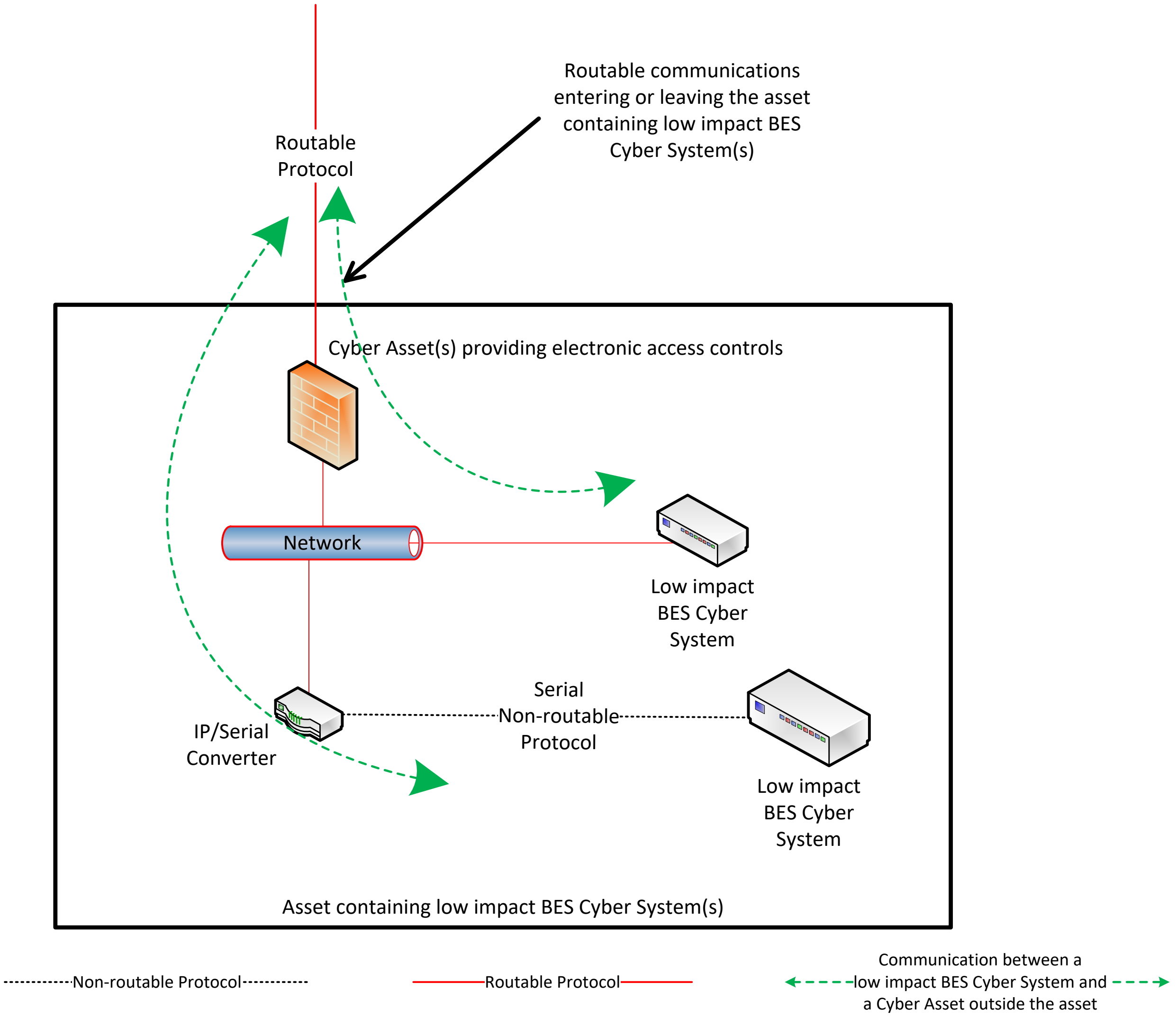
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

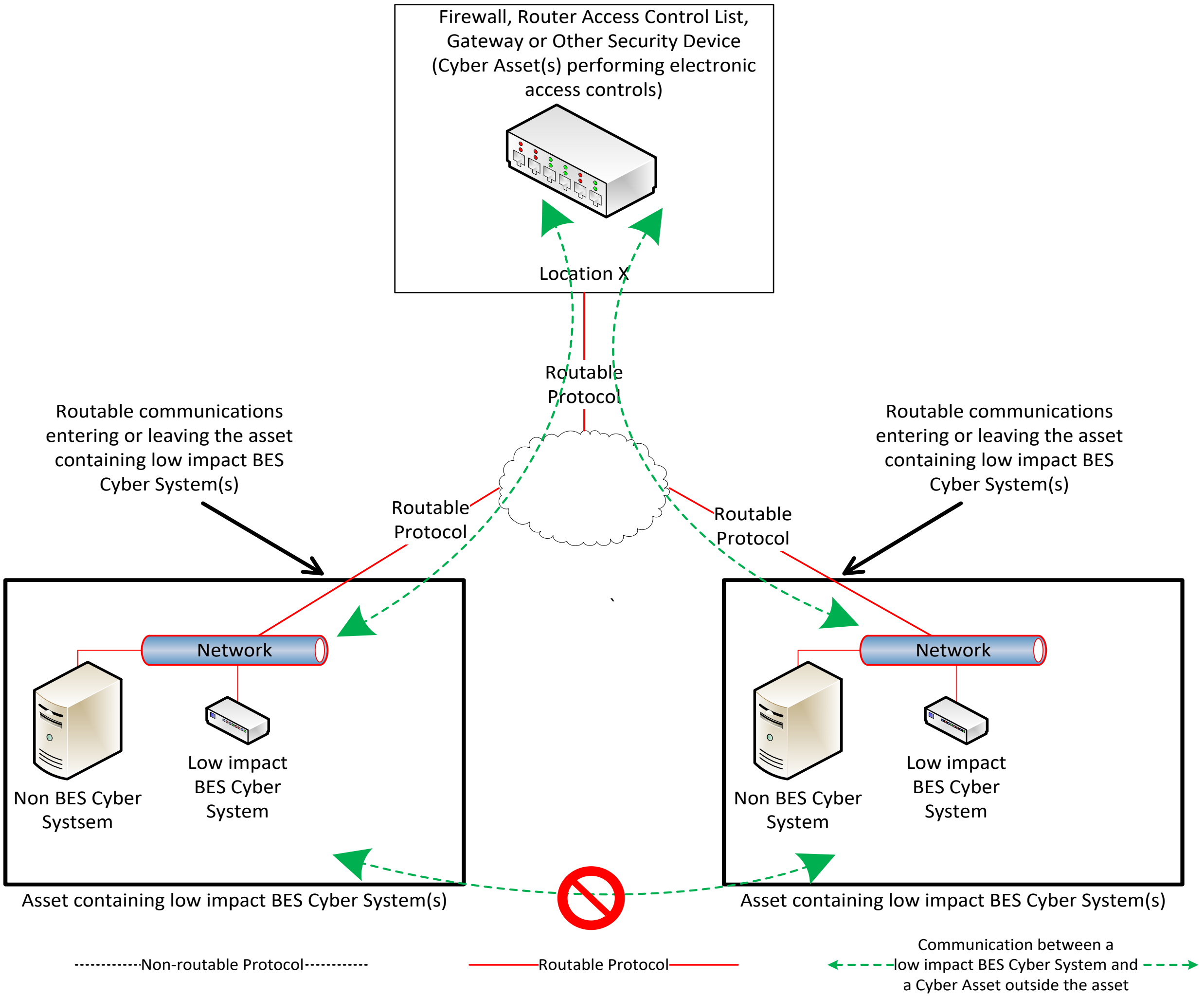
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

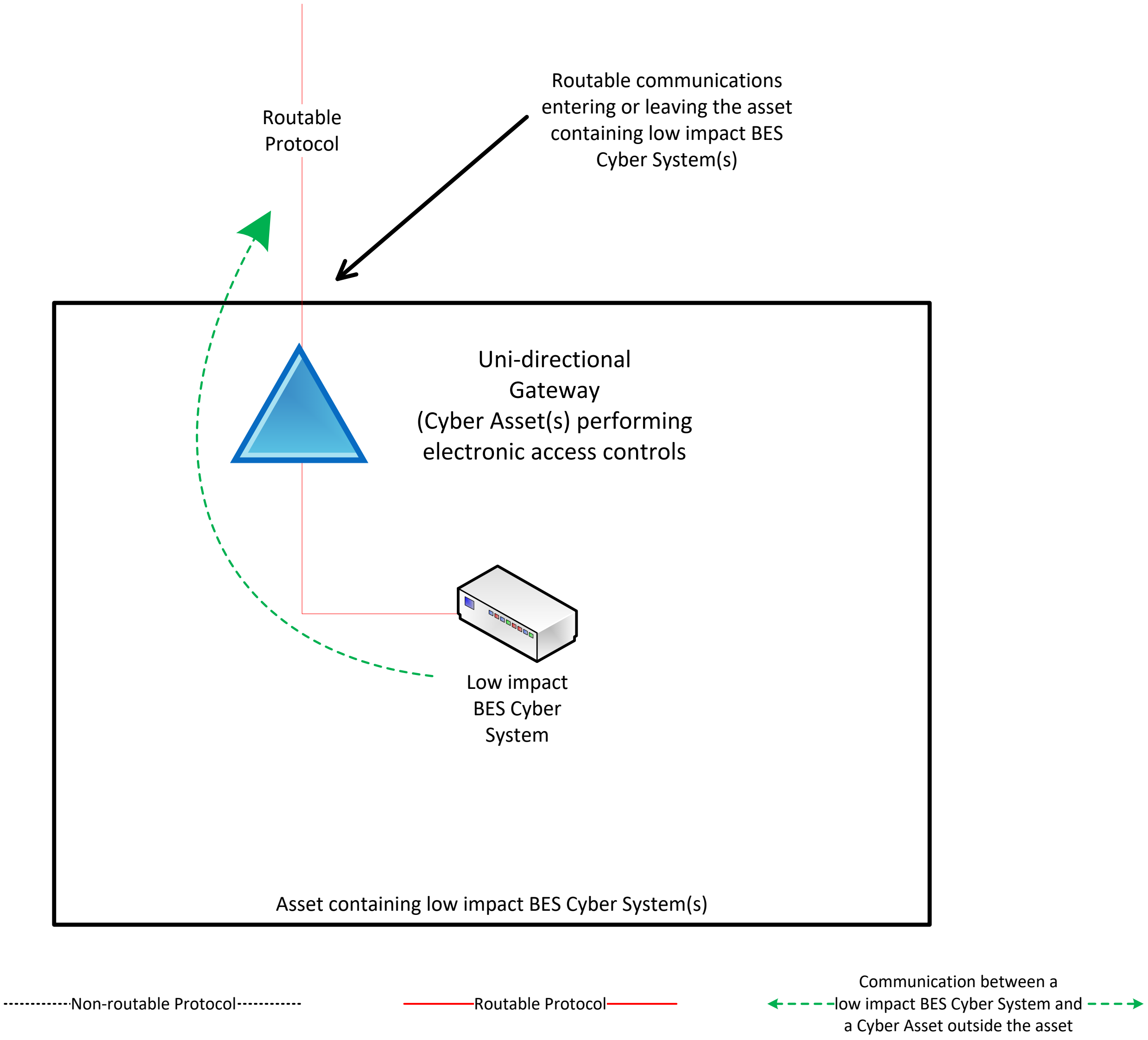
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

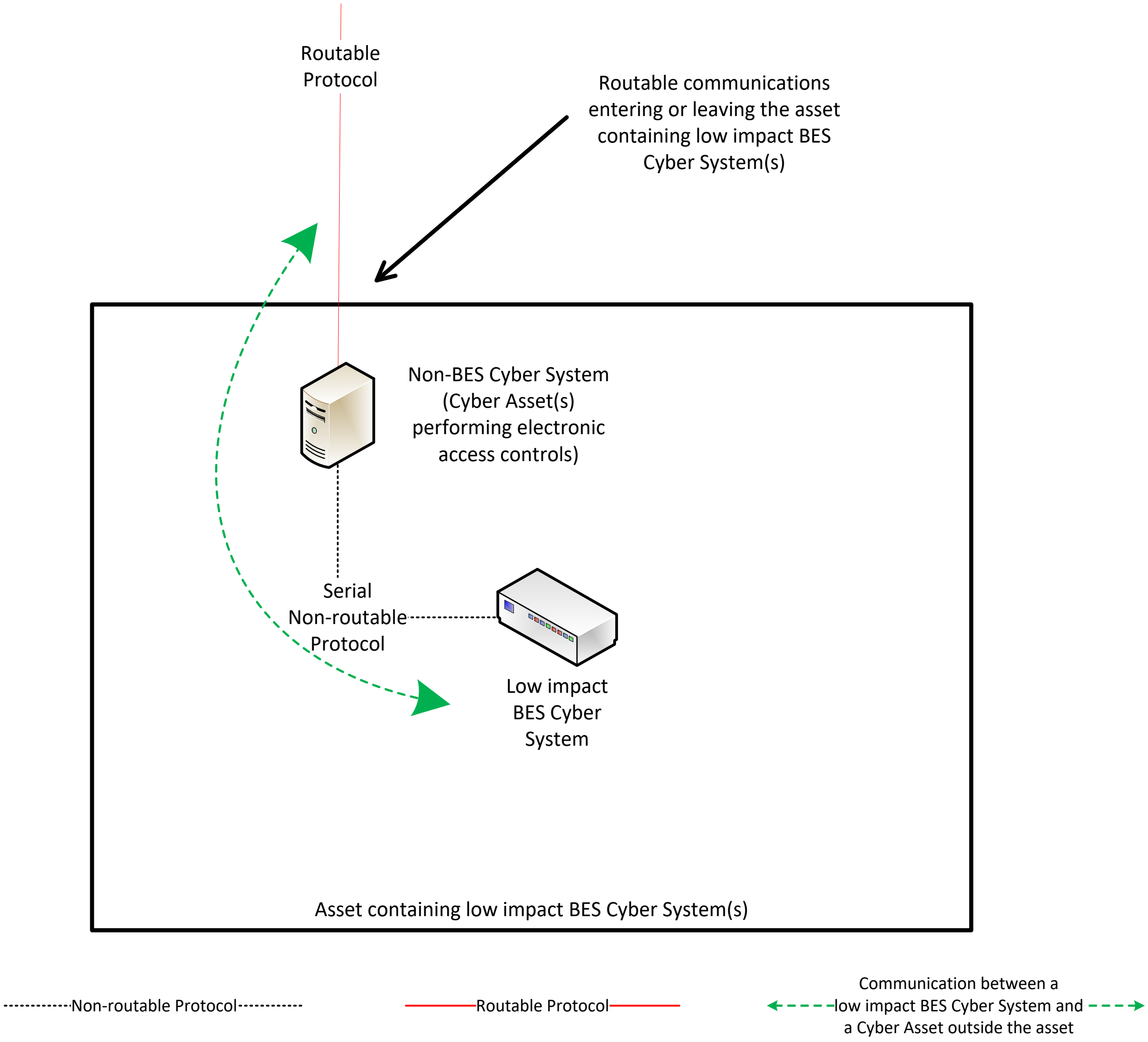
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

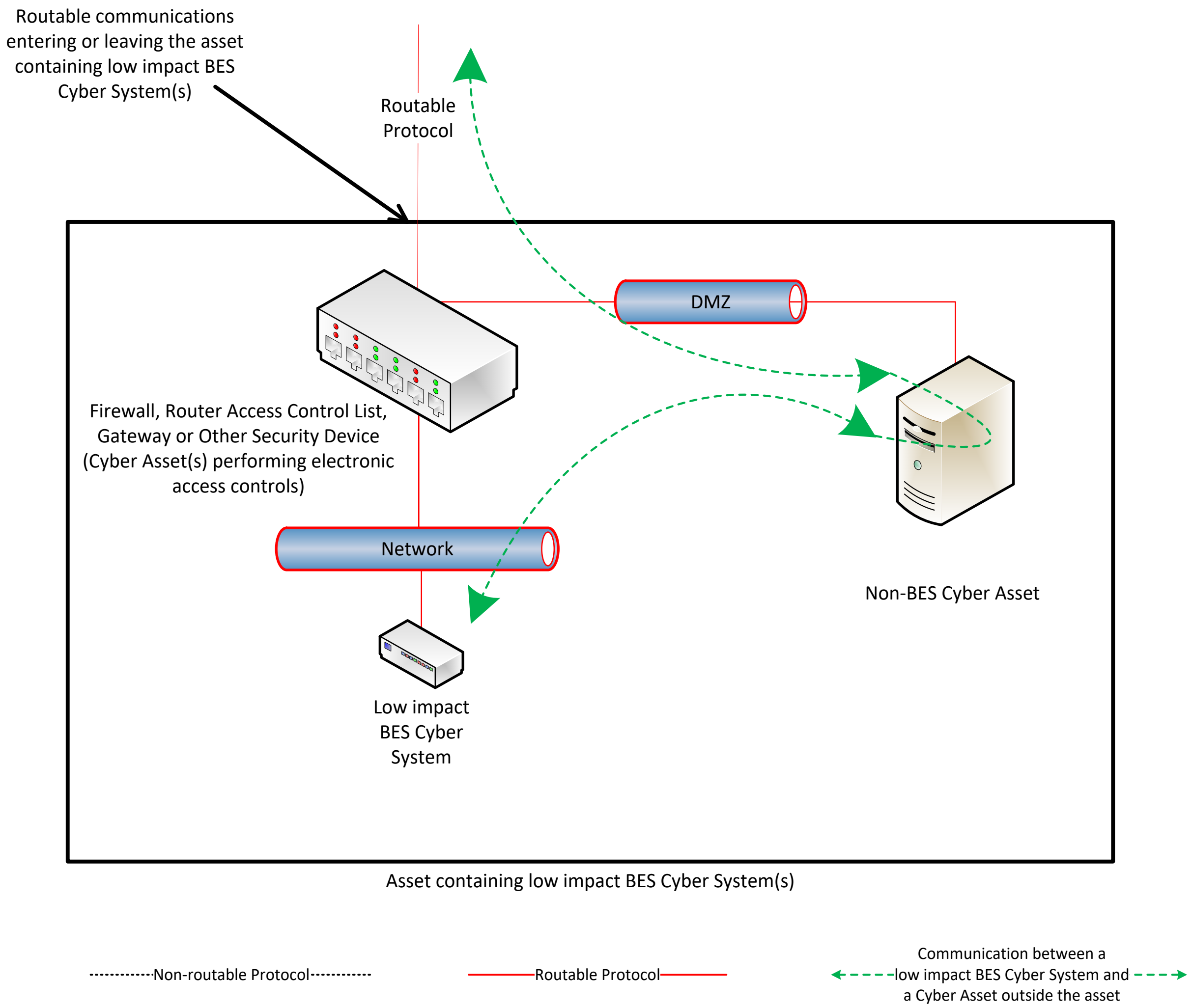
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

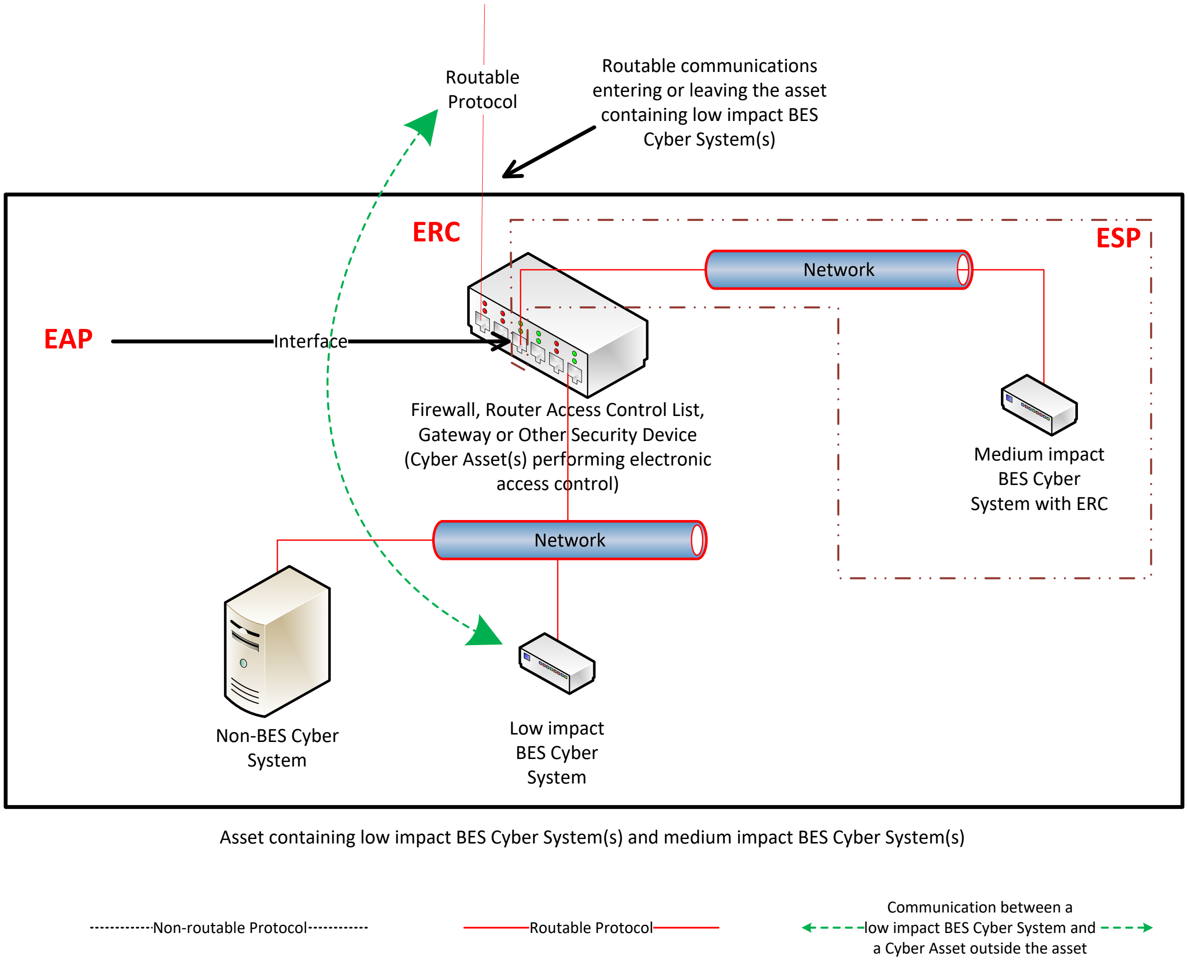
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.



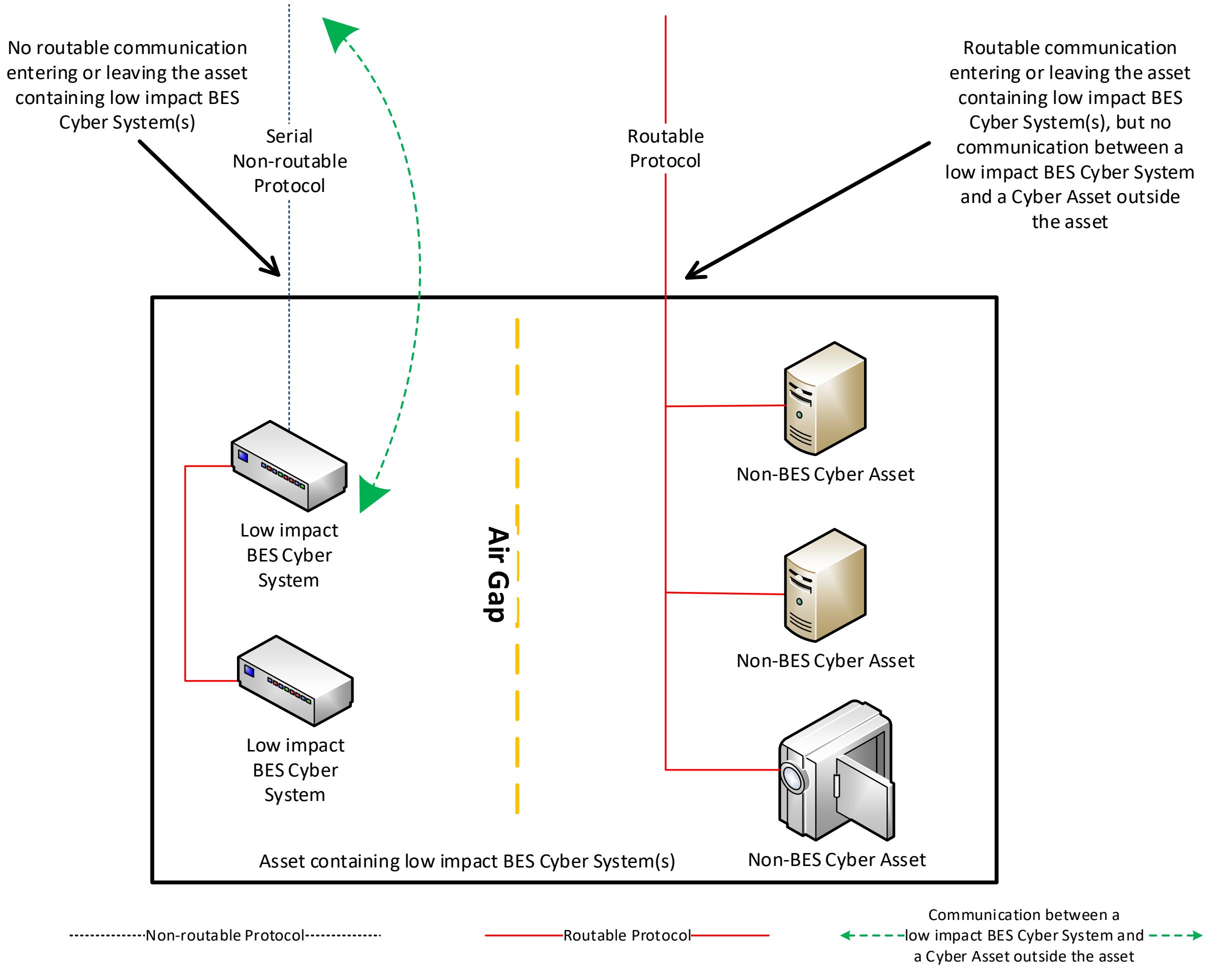
Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1. The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2. The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3. The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).

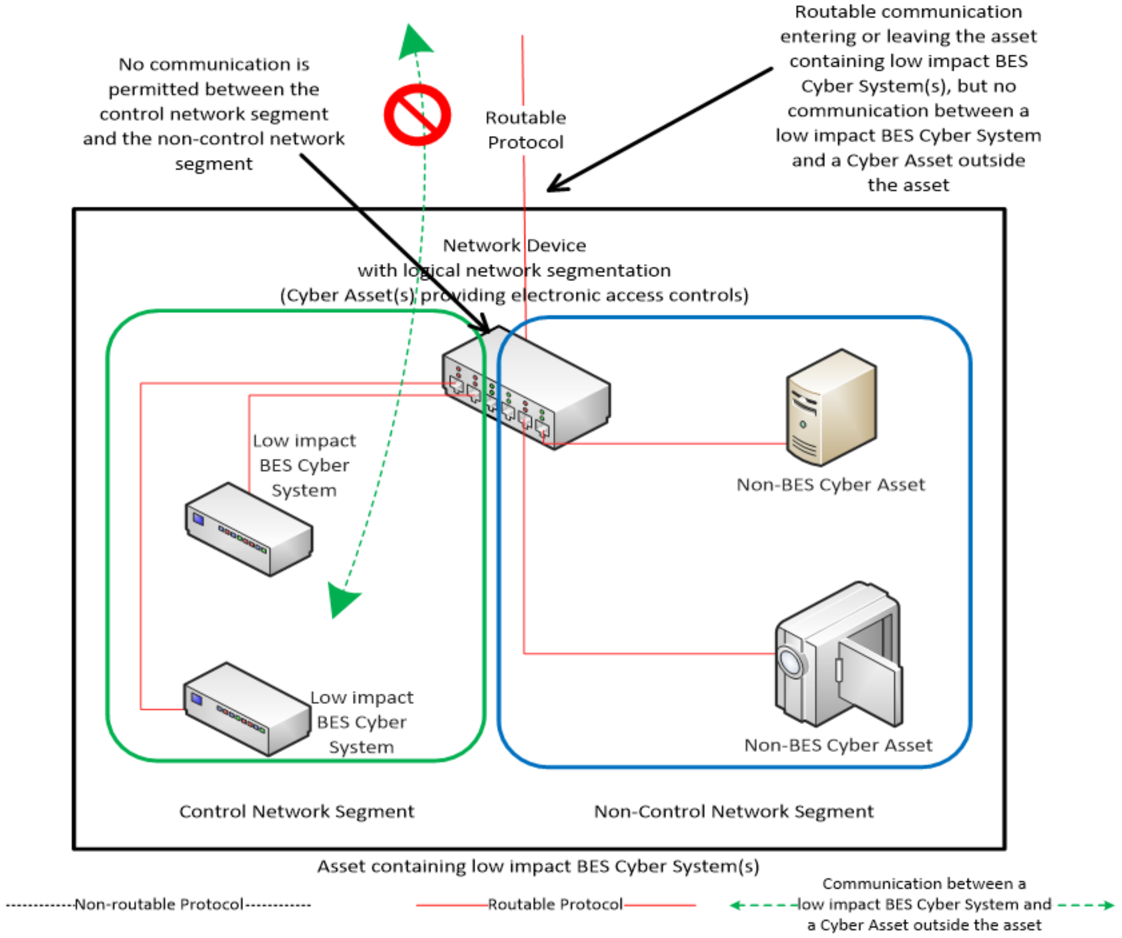
Section 1.



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

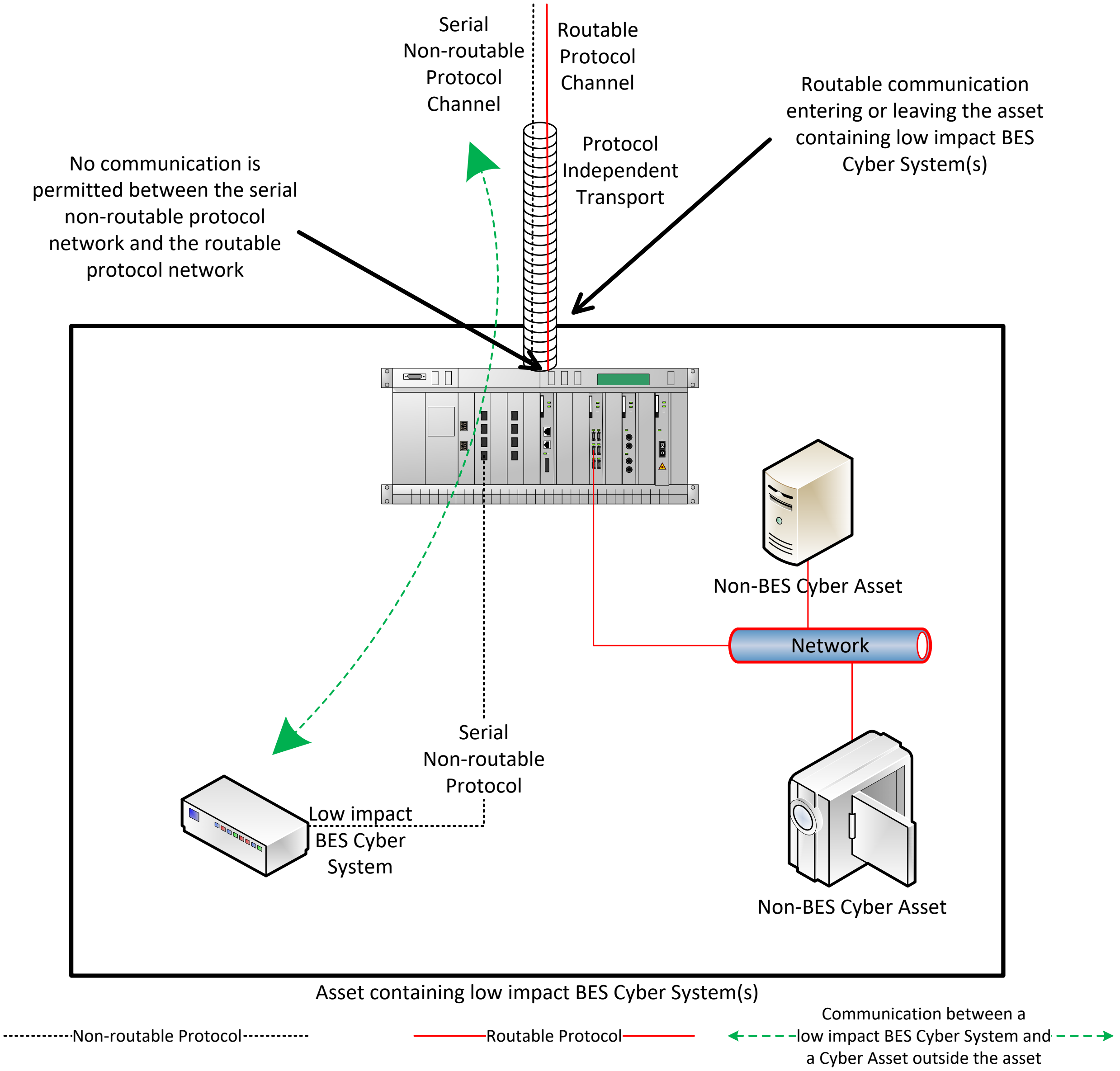
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of "controlling" inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section

5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity’s responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party’s security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of “prior to connecting the Transient Cyber Assets” is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2.1: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Section 5.2.2: The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

---

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity’s BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management’s commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious

Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for “clear lines of authority and ownership for security matters.” With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-8

February 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-004-8

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-004-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the issues identified by the V5TAG was virtualization. The V5TAG Transfer document states, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." Document for reference when reading the technical rationale that follows.

Requirement R1-R6

General Considerations

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-004-8 to align personnel and training requirements with the virtualization changes.

To enable CIP-004-8 for virtualization, the SDT added "Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part" within the Applicable Systems column of each of the Parts for Requirement R1 – Requirement R6.

Additionally, where the term BES Cyber System (BCS) was used in the requirement language, it is replaced with "Applicable Systems" to align the requirement language of each Requirement Part with the updated applicability for each Requirement Part.

Requirement R3 Part 3.5

Summary of Changes:

A CIP Exceptional Circumstance was added as an exception to “Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 through 3.4 within the last seven years” such that individuals granted authorized electronic access and authorized unescorted physical access have undergone the personnel risk assessment processes.

Change Rationale:

The SDT determined Responsible Entities cannot require personnel risk assessments for first responders prior to granting them authorized unescorted physical access during certain conditions that qualify as CIP Exceptional Circumstances.

Former Background Section from Reliability Standard CIP-004-7

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

The following conventions are used in the “Applicable Systems” column as described. High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- Medium Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- Medium Impact BES Cyber Systems with External Routable Connectivity – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- Electronic Access Control or Monitoring Systems (EACMS) – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- Physical Access Control Systems (PACS) – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-004-7

General Considerations for Requirement R1

None

Rationale for Requirement R1

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table Requirement R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets (TCA) and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, TCA and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3

General Considerations for Requirement R3

None

Rationale for Requirement R3

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new personnel risk assessment (PRA). Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4

General Considerations for Requirement R4

None

Rationale for Requirement R4

Authorization for electronic and unescorted physical access must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5

General Considerations for Requirement R5

None

Rationale for Requirement R5

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5 Part 5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement R5 Part 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the Bulk Electric System. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Requirement R6

General Considerations for Requirement R6

None

Rationale for Requirement R6

Requirement R6 requires Responsible Entities to implement a BES Cyber System Information (BCSI) access management program to ensure that provisioned access to BCSI is authorized, verified, and promptly revoked. Authorization ensures only individuals who have a need are authorized for provisioned access to BCSI. Prompt revocation of terminated individuals' ability to access BCSI helps prevent inappropriate disclosure or use of BCSI. Periodic verification ensures that what is currently provisioned is authorized and still required, and allows the Responsible Entity the opportunity to correct any errors in provisioning.

The change to "provisioned access" instead of "designated storage locations" enables the use of third-party solutions (e.g., cloud services) for BCSI. The concept of "designated storage locations" is too prescriptive and limiting for entities that want to implement file-level rights and permissions (i.e., policy based credentials or encryption keys that follow the file and the provisioned individual), which provide BCSI access controls regardless of storage location. The concept of provisioned access provides the needed flexibility for entities to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

According to Requirement R6, Part 6.1, the Responsible Entity must authorize individuals to be given provisioned access to BCSI. First, the Responsible Entity determines who needs the ability to obtain and use BCSI for performing legitimate work functions. Next, a person empowered by the Responsible Entity to do so authorizes—gives permission or approval for—those individuals to be given provisioned access to BCSI. Only then would the Responsible Entity provision access to BCSI as authorized.

Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI.

For BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet. For BCSI in electronic format, electronic access is provisioned to an electronic system or its contents, or to individual files. Provisioned physical access alone to a physical location housing hardware that contains electronic BCSI is not considered to be provisioned access to the electronic BCSI. Take, for instance, storing BCSI with a cloud service provider. In this case, the cloud service provider's personnel with physical access to the data center is not, by itself, considered provisioned access to the electronic BCSI stored on servers in that data center, as the personnel would also need to be provisioned electronic access to the servers or system. In scenarios like this, the Responsible Entity should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011-X. The subparts in Requirement R6, Part 6.1 were written to reinforce this concept and clarify access management requirements.

The periodic verification required by Requirement R6 Part 6.2 is to ensure that only authorized individuals have been provisioned access to BCSI and that what is provisioned is what each individual currently needs to perform work functions. For example, by performing the verification, the Responsible Entity might identify individuals who have changed jobs and no longer have a need for provisioned access to BCSI, and would therefore revoke provisioned access.

For Requirement R6 Part 6.3, removal of an individual's ability to use provisioned access to BCSI is considered to mean a process with the result that electronic access to electronic BCSI and physical access to physical BCSI is no longer possible from that point in time onwards using the means the individual had been given to obtain and use BCSI in those circumstances. Either what was specifically provisioned to give an individual access to BCSI (e.g., keys, local user or database accounts and associated privileges, etc.) is taken away, deleted, disabled, revoked, etc. (also known as "deprovisioning"), or some primary access is removed which prevents the individual from using the specifically provisioned means. Requirement R6 Part 6.3 acknowledges that where removing unescorted physical access and Interactive Remote Access, such as is required in Requirement R5 Part 5.1, prevents any further access to BCSI by the individual after termination, then this would constitute removal of an individual's ability to use provisioned access to BCSI. Access can only be revoked or removed where access has been provisioned. The intent is not to have to retrieve individual pieces of BCSI (e.g., documents) that might be in someone's possession (although you should if you can, but the individual cannot un-see what they have already seen).

Where no specific mechanisms are available or feasible for provisioning access to BCSI, these requirements are not applicable. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BCSI, such as when the individual is handed a piece of paper during a meeting or sees a whiteboard in a conference room. Likewise, these requirements are not applicable where provisioned electronic or physical access is not specifically intended to provide an individual the means to obtain and use BCSI. There will likely be no specific provisioning of access to BCSI on workstations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BCSI is only temporarily or incidentally located or stored there. Another example is the provisioning of access to a substation, the intent of which is to enable an individual to gain access to the substation to perform substation-related work tasks, not to access BCSI that may be located there. However, BCSI in these locations and situations still needs to be protected against unauthorized access per the Responsible Entity's information protection program as required by CIP-011-X.

The change to "provisioned access" to BCSI is backwards compatible with the previous "designated storage locations" concept. Entities have likely designated only those storage locations to which access can be provisioned, rather than any location where BCSI might be found. Both concepts intend to exclude those locations where BCSI is temporarily stored, as explained in the previous paragraph. Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of information. The removal of the term "designated storage location" does not preclude an entity from defining storage locations for the entity's access management program for authorization, verification, and revocation of access to BCSI.

Technical Rationale for Reliability Standard CIP-004-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity’s process during the tenure of employment, which may or may not be the same as the initial verification action.

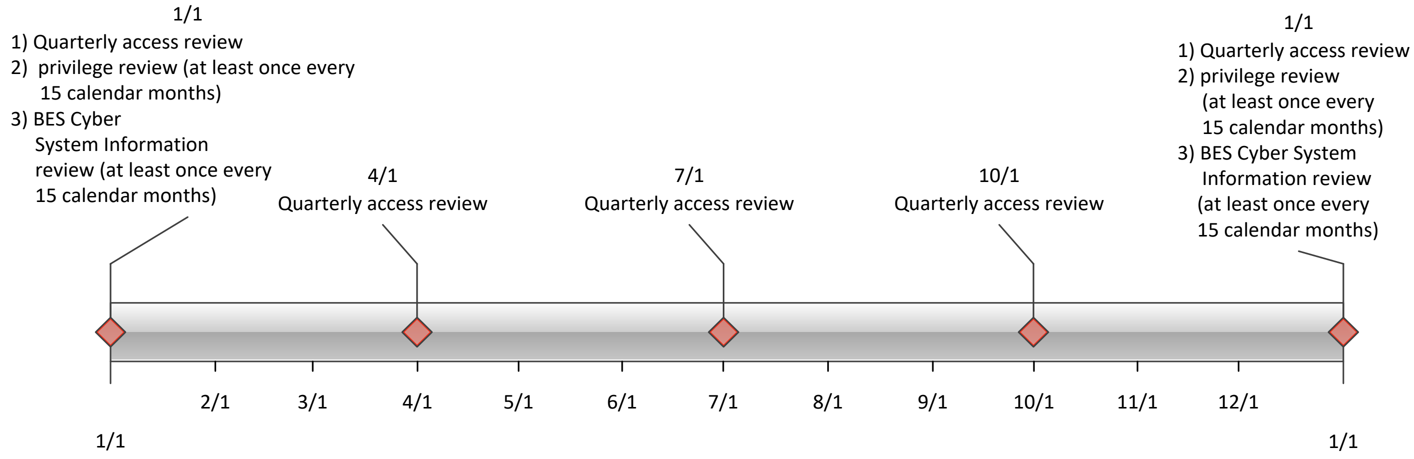
A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.



Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing “immediate” revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security – BES Cyber System Logical Isolation

Technical Rationale and Justification for Reliability Standard CIP-005-8

February 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-005-8

Introduction

This document is the technical rationale and justification for Reliability Standard CIP-005. It includes the rationale for changes in the current proposed version (CIP-005-8) as well as previous versions of the standard. The intent of this document is to provide stakeholders and the ERO Enterprise with an understanding of the revisions and the technical concepts of the Reliability Standard as well as the rationale for such revisions, both the currently proposed and historical revisions from previous versions and SDTs.

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition Advisory Group (V5TAG), which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005-8 and the definitions of Cyber Asset and Electronic Access Point (EAP) that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

Summary

The Project 2016-02 Standard Drafting Team (SDT) proposal accommodates for increasing use of virtualization and other technology innovation. The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards, but also to better position the CIP standards to be applicable to additional future technological innovation while, to the extent possible, maintaining backwards compatibility.

CIP-005-8 remains a standard concerned with controlling communications to and from BES Cyber Systems (BCS) by establishing an Electronic Security Perimeter (ESP) with increased security controls for Interactive Remote Access (IRA) and vendor remote access. However, virtualization is enabling models for network security, such as "Zero Trust", that are not network perimeter based. Therefore, in CIP-005-8 the ESP focuses on being a security model rather than a network topology-based perimeter as the only option. Securing the communications to and from BCS is the security objective, but the standard no longer prescribes "where", as in where on a network, the controls must be implemented. Innovations such as Zero Trust models are moving access control from network borders to a session level orientation and eliminating the implicit trust within a local network. Network perimeter-based ESP and EAP implementations remain a valid option and are one method for allowing only necessary communications to the Cyber

Systems within the ESP. The ESP definition has a new option that elevates it to the security objective while maintaining current state compatibility.

Another concept introduced within CIP-005-8 is Shared Cyber Infrastructure (SCI). With the introduction of hardware (servers, storage, networks) as an infrastructure fabric on top of which virtual machines, networks, and storage locations are built, the need to isolate Cyber Systems from others of different trust levels must move beyond a network-only separation. Where SCI is used in virtualized environments, a risk of side channel attacks exists. CIP-005-8 Requirement R1 mitigates this risk.

CIP-005-8 Requirement R1 Part 1.3 then restricts communications between the SCI's management plane and the data plane; Ensuring the reliability and security of network and hardware isolation configuration, as well as protections for administrative actions to create, manage, or delete VCAs.

CIP-005-8 also introduces exemptions and requirements for extending single ESPs across different Physical Security Perimeters (PSP), or "Super ESPs", often used to improve resilience and reliability by extending a flat network between virtualized infrastructures in two different locations to allow VCAs to seamlessly transfer between them.

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 General Considerations

ESP Redefined

Network border-based ESPs and EAPs remain a valid option for controlling the communications to and from BCS. However, virtualization technologies and models such as Zero Trust present equally effective methods that are not network border-based solutions. A Zero Trust model can implement more granular controls throughout a network on a per-access or per-session level.

Shared infrastructure and "Mixed Trust" Risks

For virtualized environments where SCI is used, a risk of side channel attacks exists. Virtualization allows disparate workloads of what could be differing impact or trust levels to execute on the same CPUs and share the same memory (i.e. RAM). For example, a low impact BCS that is isolated from a high impact BCS from a network communication perspective, but still shares CPU or memory with the high impact BCS, could be used to attack the high impact BCS through hardware-level vulnerabilities. Vulnerabilities (such as Spectre, Meltdown, and Rowhammer) directly relate to sharing resources and are unique risks of virtualization. Rowhammer, for example, concerns processes sharing hardware memory where repeated writing of bits in one process could flip bits in a process in adjacent physical memory. The risk of these vulnerabilities is being mitigated in CIP-005-8 by either:

- Declaring the VCAs that share CPU or memory or are within the same ESP with a BCS as associated PCAs which will require they meet the security requirements (high water marking) that include 'associated PCAs'; or
- Configuring the virtualization infrastructure to place VCAs of differing impact or trust levels into differing ESPs and configuring affinity controls to these zones such that hypervisors do not allow workloads in these differing zones to simultaneously exist or execute on the same hypervisor.

Assets with Multiple Classifications (PCA, EACMS, Intermediate System, SCI, etc.)

The definitions created to categorize Cyber Assets have historically included overlap. The definition of PCA was revised to include VCAs that share CPU or memory with a BCS. Additional definitions such as SCI and VCA will add to the possibility of additional instances of assets or systems meeting multiple definitions, such as SCI that are also EACMS.

These definitions are used in both the Applicable Systems column as well as within the requirement language. The fact that one asset or system may have multiple classifications does not pose a significant challenge as long as the Responsible Entity ensures that all requirements that pertain to ANY of the classifications are applied. In other words, if an asset or system meets both the SCI and the EACMS definition, requirements that apply to either categorization are applicable.

Requirement R1

Rationale

Requirement R1 requires implementation of an ESP for BCS permitting only necessary communication through the ESP. However, there are other network security models available (such as zero trust) that can accomplish this security objective by controlling communications end-to-end at a more granular level than a network perimeter-based model. The definitions (ESP and EAP) and the changes to R1 allow entities the flexibility to implement different models that meet the security objective, or retain their current perimeter-based implementation.

Requirement R1 Part 1.1:

Rationale

This Requirement Part requires all high and medium impact BCS and their associated PCAs be protected by an ESP. In recognition of non-perimeter based models, the language changed from “shall reside within” to “must be protected by”. Note, a PCA can now be defined by two different attributes of what they share with a BCS – not only network location, but also the sharing of CPU and memory from the underlying hypervisor(s) for VCAs. In the instance that a VCA becomes an ‘associated PCA’ from its sharing of CPU or memory with a high or medium impact BCS, that associated PCA must also be protected by an ESP.

Note that this Requirement Part applies to all high and medium impact BCS without regard to external connectivity from the local network to other networks. This allows for the identification of PCAs and the scope of TCA connectivity even on isolated networks.

Requirement R1 Part 1.2:

Rationale

This Requirement Part changed to a security objective, rather than prescribing ERC must be controlled at an EAP. Virtualization technologies introduce additional methods to isolate systems. This requirement part no longer prescribes one method of controlling communications to Applicable Systems, and opens it up for alternative solutions.

This allows for other models such as zero trust architectures. Such models are not based on controlling communications at a Cyber Asset interface located on a network boundary. Communications can be authorized by software defined policy enforcement points throughout the infrastructure. In this model, network security is less topology-based and more policy-based (configurations and settings) and can be used to granularly protect communication at an individual system or even process or resource level.

While pure zero-trust architectures are an emerging model, the objective-based requirement also allows for hybrid models of various combinations of network border-based and zero trust architectures. As technology changes, this requirement and broadened ESP definition are flexible as to how the objective is met.

The core security objective of permitting only needed communications and denying all others by no longer prescribing this must be implemented at a Cyber Asset interface on a network border (an EAP) is retained. The intent of this Requirement Part is to control the 'reachability' of the Applicable Systems; filtering network communications *before* they reach the Applicable Systems and their OS, not as part of it. This is not to discourage the use of integrated host-based firewalls to further filter network traffic to a host.

Time-sensitive communications between Protection Systems (i.e., digital relays) that use routable communication protocols is excluded. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by inserting an ESP and its controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles (sub-second response times) to protect BES assets. The SDT intent is a Responsible Entity using this technology is not expected to implement the electronic access controls in a situation where it would prohibit the proper function in the proper timeframe.

Requirement R1 Part 1.3:

Rationale

The purpose of this new Requirement Part is to permit only needed communications to and from the Management Interfaces, denying all other communications, of the systems that are providing the protection of BCS; namely SCI that is supporting an Applicable System from Part 1.1 (SCI isolates systems of different impact levels from each other) and EACMS that are enforcing an ESP. These are vital controls performing the isolation/segmentation between systems of differing impact levels, and warrant protection of the Management Interface that could be used to compromise them.

For the EACMS portion, a firewall that is enforcing and ESP, as well as a network switch configured with VLANs to isolate and segment traffic are intended to be included and have their Management Interfaces protected.

The 'per system capability' is included in this Part in recognition that some Management Interfaces, such as "ILO" interfaces, may do inbound but not outbound traffic controls.

Requirement R1 Part 1.4:

Rationale

Requirement R1 Part 1.4 was written to address the issue of "Super ESPs" with high or medium impact BCS at Control Centers that extend a single ESP beyond one PSP. This often applies to virtualized Control Center environments that implement network adjacency to allow workloads to automatically move from one physical location to another to increase BCS resiliency between primary and backup Control Centers.

Data traversing communication links between the two PSPs must be protected to preserve its integrity and confidentiality. This works in conjunction with the new 4.2.3.3 exemption in the CIP standards that exempts the Cyber Systems associated with such communication links since the data is required to be protected per this requirement. Also, the former CIP-006-6, Requirement R1, Part 1.10 has been removed and incorporated into this new 1.4 requirement part; consolidating the protections of an ESP and its components that extend outside of a PSP within one standard.

Communications equipment associated with communications links (e.g., equipment belonging to carriers) is exempted from the CIP standards with the 4.2.3.2 exemption, however that only applies to equipment between discrete ESPs. However, in this extended ESP situation where a single ESP spans different sites or PSPs, that exemption does not apply and the potential exists for data to traverse a connection that uses third-party communications equipment that is unprotected inside an ESP; hence the need to enforce confidentiality and integrity controls (such as encryption) on the data that traverses PSPs while within the same ESP to isolate any protected data from access through the communications equipment.

This consolidation also incorporates cabling and non-programmable communication components that are not PSP-protected, intending to protect data moving across the state as well as data traversing cabling that crosses the hall outside of the PSP. Note: the language specifically exempts the data that falls under CIP-012 Requirements in order to avoid the potential for double jeopardy as well as the time-sensitive protection or control functions as described in CIP-005-8 Requirement R1 Part 1.1 above.

Requirement R1 Part 1.5:

Rationale

The SDT included “SCI identified independently supporting an Applicable System above” to the scope of the requirement part to ensure that controls regarding Dial-up Connectivity are also applicable to VCAs and SCI; and, ‘technical feasibility’ has been replaced with the ‘per system capability’.

Requirement R1 Part 1.6:

Rationale

Known or suspected malicious communication detection is specific to Internet Protocol (IP) based traffic that enters or leaves the required ESP. Products available to implement this malicious communication detection are usually based on IP traffic (as defined in RFC 791 and upon which TCP and UDP reside). Requirement applicability was changed to BCS instead of EAPs; lifting it to an objective level and keeping it from being a prescriptive ‘where’ that forces certain architecture.

Requirement R2:

General Considerations for Requirement R2.

External Routable Connectivity (ERC) and Interactive Remote Access (IRA)

The ERC and IRA definitions have been updated in order to:

1. Incorporate new models such as Zero Trust where a security perimeter is not necessarily a network perimeter and ESP’s become very granular based on policies that can be established at “people to resource” levels rather than IP address levels.
2. Recognize those Cyber Systems that are of an increased risk due to their “reachability” via ERC and that have IRA available to them even if they are serial-only, non-routable devices.
3. Continue to limit scope of Requirement Parts to BCS with ERC and not those that have connectivity such as non-routable serial leased circuits.

The V5TAG transfer document in the SDT’s scope include the issue of a BES Cyber Asset (BCA) that only speaks non-routable protocols over a serial port. These BCAs are not connected to a network with a routable protocol themselves and therefore can be considered to not be within an ESP and thus not have ERC or IRA. However, these BCAs can have interactive user access using those serial connections. The SDT’s intent is to clarify that IRA can occur to a device with only a serial, non-routable connection through IP-to-serial conversions and be subject to CIP-005-8 Requirement R2. For example, the intent is to clearly cover situations where a serial-only, non-routable BCA, such as a digital relay in a substation, has its serial communication from a ‘console port’ converted to IP or other routable protocols thus allowing IRA from users outside the substation to use a routable protocol to interact with the serial device and to require the CIP-005-8 Requirement R2 protection for that IRA.

The SDT removed the requirement-style language “The Intermediate System must not be located inside the Electronic Security Perimeter” from the Intermediate Systems definition in favor of a clarified objective in CIP-005-8 Requirement R2 that all IRA must be *through* an Intermediate System. Requirement R2 Part 2.6 was added to objectively address the location of the Intermediate System.

See the “*CIP Definitions and Exemptions Technical Rationale*” document for further explanation of the changes to the R2 related definitions.

The scoping of R2 has been clarified to “all IRA and vendor remote access” and the applicability of several Requirement Parts was updated for virtualized environments to include SCI supporting an Applicable System within the Part.

Requirement R2 Part 2.1:

Rationale

Applicable Systems was updated to include SCI to ensure the same safeguards for remote access methods exist for SCI supporting an Applicable System within the Part as they do for the high and medium impact BCS and associated PCA hosted on that SCI. Backwards compatibility is retained for entities that do not use SCI.

The requirement language was simplified, and definitions for IRA and Intermediate System have been updated. Please note that the definition of IRA was changed to include serial communications that are converted to routable protocols. This change maintains backwards compatibility except where serial connectivity and routable protocol conversion is being used for IRA.

Requirement R2 Part 2.2:

Rationale

The “Applicable Systems” scope was changed to “Intermediate Systems used to access Applicable Systems of Part 2.1”. This clarifies this requirement is associated with the IRA communications between an Intermediate System and the remote clients, as opposed to between the Intermediate System itself. This is important so that it does not require encryption through the ESP to the BCS thereby hindering monitoring and inspection.

The requirement was changed from a specific technical-based requirement for encryption to an objective-based requirement to protect confidentiality and integrity of the IRA session between the Intermediate System and the remote client (with encryption as a primary example). The proposed language accounts for the possibility that other equally effective methods could be developed and deployed. This objective also keeps methods from being used that are merely obfuscation methods (XOR, ROT13, etc.) or deprecated encryption methods (DES with 56-bit keys) that no longer meet the objective to protect the confidentiality and integrity of the IRA session.

The changed requirement is backwards compatible except where deprecated encryption methods are in use.

Requirement R2 Part 2.3:

Rationale

The Applicable Systems was changed to “Intermediate Systems used to access Applicable Systems of Part 2.1”. This clarifies this requirement is associated with the Intermediate System itself, and where the requirement for multifactor authentication should be applied (multi-factor authentication to the Intermediate System).

Requirement R2 Part 2.4 – 2.5:

Rationale

The Applicable Systems section of this requirement was updated to include SCI for instances where vendor remote access is allowed to the SCI. The Applicable Systems were also modified such that only those with vendor remote access are in scope and thus need to have one or more methods for CIP-005-8 Requirement R2 Parts 2.4 and 2.5.

The requirements themselves have not changed.

Requirement R2 Part 2.6:

Rationale

This is a new requirement that applies to Intermediate Systems. The intent of this new requirement is to further protect the BCS from the Intermediate System by reducing the attack surface between the two. Intermediate Systems have an externally accessible interface that may be used by external parties such as vendors or entity support staff using IRA across an Internet connection to support a remote site. Since Intermediate Systems by nature provide IRA from a less-trusted network and are accessible from yet-to-be authenticated users (in order to authenticate them), a degree of separation from the higher-trust systems they are protecting is necessary in case the Intermediate System is compromised. Previously, this risk was addressed within the glossary definition of Intermediate System ("…must not be located inside the ESP") instead of within an actual requirement. The SDT removed this from the definition and included a security objective in CIP-005-8 Requirement R2 Part 2.6 to require that routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.

It is important to note that a virtualized Intermediate System (VCA) hosted in such a way that it can share CPU and memory with a BCS will also meet the definition of PCA and become an 'associated PCA' of the BCS. Therefore, CIP-005 R1.1 requires it be within the ESP, in conflict with this requirement. This is by design, and thus a VCA performing the function of an Intermediate System must not share CPU or memory with the BCS it is controlling access for. This is due to the access granted to the less trusted side of the Intermediate System and the risk is has for side-channel hardware-based attacks to the BCS. Entities must therefore use affinity rules or some other means to keep Intermediate System VCAs from sharing the same CPU and memory as the Applicable Systems they are providing IRA to.

Requirement R3

Rationale

The Applicable Systems section of CIP-005-8 Requirement R3 was updated to include SCI to ensure the same safeguards for vendor-initiated remote connections exist for the applicable SCI. Backwards compatibility is retained for entities that do not currently use SCI.

Former Background Section from Reliability Standard CIP-005-7

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BCS and require a minimum level of organizational, operational and procedural controls to mitigate risk to BCS.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BCS. For example, a single training program could meet the requirements for training personnel across multiple BCS.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:
Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

Technical Rationale for Reliability Standard CIP-005-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The ESP serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e. system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the “first line of defense within an Industry Control System (ICS) network environment”. The compromise of those devices that control access management could provide an outsider the “keys to the front door” of the ESP where BES Cyber Systems reside. An intruder holding the “keys to the front door” could use those “keys” to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability

Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks*"[1].

NERC's final report on "*Cyber Security Supply Chain Risks*", states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks*" that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

---

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.

But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Physical Security of BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-006-7

February 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-006-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-006-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-006-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-006-7 to shorten applicability statements within the body of CIP standards by replacing some terms with the defined acronym for that term:

- "BCS" has replaced "BES Cyber System".
- "ERC" has replaced "External Routable Connectivity".
- "PSP" has replaced "Physical Security Perimeter".
- "PACS" has replaced "Physical Access Control Systems".

Requirement R1

Rationale

<u>Per System Capability vs Technical Feasibility</u>:
Requirement R1 Part 1.3: The SDT chose to remove the reliance on a Technical Feasibility Exception in favor of the updated term "per system capability."

<u>Consolidation</u>:
Requirement R1 Part 1.10: The SDT deleted Requirement R1 Part 1.10 from CIP-006-7 because it is incorporated into CIP-005-8 Requirement R1 Part 1.4.

Requirement R2

Rationale

The SDT has include the CIP Exceptional Circumstances within the main R2 requirement text so that it applies to all requirement parts.

Former Background Section from Reliability Standard CIP-006-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-006-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-006-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the PSP.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more PSPs, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the PSP to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the PSP. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a PSP (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any PSPs protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — System Security Management

Technical Rationale and Justification for Reliability Standard CIP-007-7

February 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-007-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-007-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-007-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale.pdf" for reference when reading the technical rationale that follows.

Requirement R1

General Considerations for Requirement R1

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-007-7 for virtualization, the SDT added "SCI supporting an Applicable System in this Part". This approach keeps the SCI applicability parallel to each existing variant of Applicable Systems in the same Requirement Part (i.e. Medium impact BCS vs. Medium impact BCS with External Routable Connectivity (ERC) vs. Medium impact BCS at Control Centers etc.)

Change Rationale Requirement R1:

The SDT has changed the name of the R1 table to "System Hardening" to more clearly reflect the security objective of the entries in the table which is to harden the applicable systems through limiting access to logical and physical ports, and to control where certain VCAs can instantiate through host affinity rules.

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCA.

Change Rationale Requirement R1 Part 1.1: Requirement R1 Part 1.1 requires "disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. The SDT updated the Requirement Part language to be more objective concerning routable protocol "ports and services". The objective is to reduce the attack surface on an applicable system preventing any unnecessary accessibility to the system using routable protocols. TCP/UDP port numbers are at times the best way to track this accessibility, at other times documenting enabled services is better. For example, hardening network accessibility in the physical underlay of SCI between hypervisors may be performed at a virtualization *services* level; turning off or disabling virtualization services that are not needed, rather than documenting the often proprietary and dynamic port numbers which may be of little value. However, in the overlay where an entity may be hosting a database server VCA on a virtual network, it may be easier to show that network accessibility is limited to two open ports and the uses of those ports and that all others are disabled or blocked. The SDT has moved to this objective language to avoid attempts to prescribe the best way to document network accessibility in all the various scenarios and implementations. In addition, it is limited to routable protocol network accessibility such that non routable network communications (e.g., SAN over Fiber Channel) do not fall within scope of the Requirement Part.

The SDT added the clarifier "on each Applicable System" to indicate that the intent of this requirement is for an entity to perform the configuration actions on each Applicable System, hardening the system from its routable protocol network peers (e.g., east/west traffic within an ESP) rather than having a single method such as an EAP network firewall rule that would disable such accessibility for a group of Applicable Systems.

The SDT chose to remove the reliance on a Technical Feasibility Exception (TFE) in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE. The 'per system capability' also allows for devices that have no provision for disabling logical ports or services, such as some firmware-based devices with very limited configuration capabilities.

Note that the Measures language has been updated to retain backwards compatibility.

Change Rationale Requirement R1 Part 1.3:

Requirement R1 Part 1.3 is a new requirement intended to apply host affinity controls to SCI that supports the Applicable Systems listed. The risk associated with this SCI is such that it may host VCAs of different impact categorizations and requires additional hardening controls to mitigate the risk of VCAs of different impact from sharing the same CPU and memory due to the risks of hardware-based vulnerabilities.

Note that the SCI definition covers only those portions of entity's virtualization infrastructure that support systems of differing impact levels. As VCAs that share the same CPU or memory with any part of the highest rated BCS are already PCAs (and thus share the same impact categorization), this requirement is only needed to cover instances where different impact categorizations are supported. This may occur when part of the same SCI supports different BCS and the entity does not wish to high watermark all the BCS together.

For example, this requirement would apply where the same SCI supports both a BCS with a high impact categorization on one part of a virtualization cluster, and a different BCS with a low impact categorization on a different part of the virtualization cluster. The proper use of host affinity controls would not require the BCS with the low impact categorization to be considered an "associated PCA" of the high as long as the new controls for SCI are in place, such as affinity controls.

Requirement R2

Change Rationale Requirement R2:

The SDT chose to include the "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA.

The SDT made conforming changes where necessary with Requirement R2 to remove reliance on the Cyber Asset term, choosing to reference the Applicable Systems instead.

Additionally, the SDT chose to insert the word "cyber" as a clarifier to security patches for consistency with the term used in R2.1.

Backward Compatibility

CIP-007-7 Requirement R2 retains backward compatibility for entities that do not utilize SCI.

The SDT intends that entities take full advantage of their virtualization infrastructure in order to ease the overhead associated with patch management. While many of the entity's existing processes will remain the same, (such as those associated with tracking the source of cyber security patches, evaluation of the applicability of available patches and mitigation plans for those applicable patches that cannot be installed) new or modified processes around the installation of patches can be used (for example, parent images, remediation VLANs, etc.)

Parent Images

One of the interesting nuances of virtualization is the concept of parent/child relationships.

Some VCAs utilize a "parent image" type methodology where the specific VCA software and operating system is merely a child instance of a parent image. In such cases, the application of cyber security patches to the parent image also applies the same changes to any children of that image. As there may be many child instances, the administrative overhead associated with patching of those instances can be greatly reduced.

Dormant Instances

There are times when VCAs are not being used and are idle. Physical instances of the assets are always left up and running in order to receive applicable patches, software updates, configuration updates, etc.

Leveraging the built in virtualization features allows idle resources to be reassigned to tasks at hand without incurring additional overhead of tracking which dormant virtual instances require patching. Dormant virtual instances are just files with the saved state of the VCA. Dormant instances are not VCAs themselves nor Applicable Systems until they become active instances again.

Where a dormant virtual instance is also the child instance of a parent image, the application of security patches to the parent image will also make the same changes automatically when needed to any out of date dormant child virtual instances when they are restarted.

In most cases, a dormant virtual child instance is made active again on a remediation type network where any missing security patches (compared to the parent image) are automatically applied before it is placed back into active service.

Saved Images

Similar to dormant child images, saved child images or snapshots may be also used as functional backups for CIP-009 purposes in order to provide fast restoration and better availability. If an active VCA becomes corrupted, a saved image can be made active where the application of any missing security patches (compared to the parent image) can be automatically applied, through remediation, before being placed back into active service.

Requirement R3

Change Rationale Requirement R3:

The SDT chose to modify the name of the Table in R3 from Malicious Code Prevention to the term used by the National Institute of Standards & Technology (NIST), Malicious Code Protection, as that more accurately clarifies the security objective of protecting BCS from malicious code.

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA.

Requirement R4

Change Rationale Requirement R4:

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA.

Change Rationale Requirement R4 Part 4.1:

The SDT determined the entire structure of the "at the BCS level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)" language could be simplified to "per system capability" since the Applicable Systems column clarifies what systems are included.

Additionally, the SDT chose to insert the word "security" as a clarifier to which events are to be logged.

Change Rationale Requirement R4 Part 4.2:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the "Cyber Asset" term, as well as the ambiguity that would have existed if the term "BES Cyber System" were left in place while the Applicability Column included SCI.

Change Rationale Requirement R4 Part 4.3:

The SDT also chose to remove the reliance on a TFE from Part 4.3 in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

Requirement R5

Change Rationale Requirement R5:

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement part in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCAs.

Change Rationale Requirement R5 Parts 5.1, and 5.6 – 5.7:

The SDT chose to remove the reliance on TFE in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

Change Rationale Requirement R5 Part 5.5:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the "Cyber Asset" term, replacing it with a reference to the Applicable Systems.

Former Background Section from Reliability Standard CIP-007-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-007-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-007-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

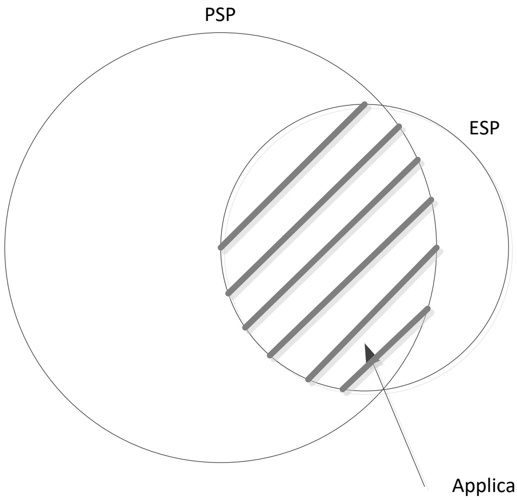
- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:

Location of Nonprogrammable Communication Components



Applicability of CIP-007-6 R1, Part 1.2 for
Nonprogrammable Communication Components

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as “at next scheduled outage of at least two days duration.” “Mitigation plans” in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:
Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.
Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.
It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.

- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security – Incident Reporting and Response Planning

Technical Rationale and Justification for Reliability Standard CIP-008-7

February 2022

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-008-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-008-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 – Requirement R4

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-008-6 to align incident reporting and response planning requirements with the virtualization changes by adding "SCI supporting an Applicable System in this Part" to each of the Parts in Applicable Systems for Requirement R1 – Requirement R4.

Requirement R4

Rationale

The Project 2016-02 SDT made updates to reflect the change from the National Cybersecurity and Communications integration Center (NCCIC) to its successor organization Cybersecurity & Infrastructure Security Agency (CISA), and deleted the historical footnote in favor of deference to the Requirement language, which already states "or their successors".

Former Background Section from Reliability Standard CIP-008-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:
Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

Medium Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

Technical Rationale for Reliability Standard CIP-008-6

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-6. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-008-6 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 19, 2018, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 848. In this Order FERC directed the North American Electric Reliability Corporation (NERC) to "develop and submit modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access and Control or Monitoring System (EACMS)." (Order 848, Paragraph 1)

In response to the directive in Order No. 848, the Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require Responsible Entities to implement methods augmenting the mandatory reporting of Cyber Security Incidents to include: "(1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report included specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT)." (Order 848, Paragraph 3)[1]

New and Modified Terms Used in NERC Reliability Standards

CIP-006-6 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms:

Cyber Security Incident

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises, or attempts to compromise the, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or
- Disrupts, or attempts to disrupt, the operation of a BES Cyber System.

In response to FERC Order 848, Paragraph 1, the SDT modified the Cyber Security Incident definition to include Electronic Access Control or Monitoring Systems (EACMS) associated with high or medium impact BES Cyber Systems, in response to the Order.

---

[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

The addition of high and medium impact BES Cyber Systems considers the potential unintended consequences with the use of the existing definition in CIP-003-7. It also provides clarity that only low impact BES Cyber Systems are included within the definition. ESP or EACMs that may be defined by an entity for low impact BES Cyber Systems are not part of the definition.

An attempt to disrupt the operation of a BES Cyber System is meant to include, among other things, a compromise of a single BES Cyber Asset within a BES Cyber System. For example, malware discovered on a BES Cyber Asset is an attempt to disrupt the operation of that BES Cyber System.

Reportable Cyber Security Incident
A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BES Cyber System; or
- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber Systems.

The Reportable Cyber Security Incident definition was modified to comply with FERC Order 848. In response to Paragraph 54 of the Order, the SDT modified the definition to include incidents that compromised or disrupted an ESP or an EACMS. The team also added the qualifying clause for “A BES Cyber System that performs one or more reliability tasks of a functional entity” to clarify what was compromised or disrupted, thus not extending the scope to Protected Cyber Assets (PCAs). In response to comments, the SDT left the entire definition of BES Cyber system in Reportable Cyber Security Incident to provide clarity.

It is also important to understand the relationship between the two definitions, the requirement language, and how they work in concert to classify events and conditions at varied levels of significance as the Registered Entity executes its process and applies its defined criteria to determine if reporting is required.

Electronic Access Control or Monitoring Systems (EACMS)
The drafting team spent significant time discussing this topic among its members, through industry outreach, and with FERC staff. The team believes by not specifically referencing the five functions in Order 848, we have reduced complexity and made compliance with the Standard achievable. The drafting team asserts that the five functions are equivalent to the current definition of EACMS in the NERC Glossary of Terms. If entities have questions about application of the EACMS definition, the drafting team advises entities to discuss those questions directly with NERC.

Requirements R1, R2, and R3

General Considerations for Requirement R1, Requirement R2, and Requirement R3

FERC Order 848, Paragraph 1, directs modifications to Reliability Standards to require reporting of incidents that compromise, or attempt to compromise a responsible entity’s ESP or associated EACMS. The intent of the SDT was to minimize the changes within CIP-008 and address the required modifications. To do this, the SDT added “and their associated EACMS” to the “Applicable Systems” column for Requirements R1, R2, and R3.

To add clarity to “attempts to compromise,” the drafting team created Part 1.2.1 to require entities to establish and document their process to include criteria to evaluate and define attempts to compromise. This requirement maps to Requirement 4 Part 4.2, which requires entities to use that entity-defined process for determining which incidents entities must report.

The use of the language describing Cyber Security Incident(s) as being “an attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the ‘Applicable Systems’” column for the Part is meant to clarify which Cyber Assets are in scope for attempts to compromise reporting by entities. This language is used throughout the standard.

Moving Parts of Requirement R1 to Requirement R4

To minimize the changes to Requirement R1, the SDT created Requirement R4 and consolidated all the CIP-008-6 reporting requirements. The SDT deleted Requirement R1 Part 1.2 reporting requirements from CIP-008-5, and moved them to Requirement R4 for this purpose.

Inclusion of "Successor Organizations" throughout the Requirement Parts

The SDT recognizes that organizations are constantly evolving to meet emerging needs, and may re-organize or change their names over time. The ICS-CERT has completed its name change to the National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems. The E-ISAC previously re-branded its name and may again in the future. By following Requirement R4 references to E-ISAC and NCCIC with "or their successors" the SDT is ensuring that Requirement R4 can be implemented even if the names of E-ISAC and NCCIC change or a different agency takes over their current roles.

Requirement R4

General Considerations for Requirement R4

Requirement R4 is a new requirement focused on mandatory reporting of Reportable Cyber Security Incidents and includes attempts to compromise systems in the "Applicable Systems" column. Previously, CIP-008-5 defined reporting requirements for Reportable Cyber Security Requirements (Requirement R1 Part 1.2) only.

Required Reportable Incident Attributes

Requirement R4.1 specifies that initial notifications and updates must include three attributes: 1) functional impact, 2) attack vector used, and 3) level of intrusion achieved or attempted. These attributes are taken directly from the Order. (FERC Order No. 848, paragraph 89).

The SDT understands that some or all of these attributes may be unknown at time of initial notification. To account for this scenario the SDT included "to the extent known" in the requirement language. There is an expectation that update reporting will be done as new information is determined or unknown attributes become known by the entity. There could be cases, due to operational need, that all the attributes may never be known, if this case presents itself that information should be reported.

Methods for Submitting Notifications

Requirement R4 Part 4.2 allows responsible entities to submit notification using any method supported by E-ISAC and NCCIC. The SDT did not prescribe a particular reporting method or format to allow responsible entities' personnel to focus on incident response itself and not the method or format of reporting. It is important to note the report must contain the three attributes required in Requirement R4 Part 4.1 as they are known, regardless of reporting method or format.

Notification Timing

Requirement R4 Part 4.2 specifies two timelines for initial notification submission; one hour for Reportable Cyber Security Incidents; and end of next calendar day for attempts to compromise systems in the "Applicable Systems" column. Paragraph 3 of FERC Order No 848 directly states that reporting deadlines must be established. Paragraph 89 further states that "timelines that are commensurate with the adverse impact to the BES that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES."

- *Reportable Cyber Security Incidents* – The SDT wrote Requirement R4 Part R4.2 to use a one hour deadline for reporting of these events because incidents in this category include successful compromise of ESP(s), EACMS, or BES Cyber System(s). One hour is referenced directly in FERC Order No 848 paragraph 89 and is also the current reporting requirement in CIP-008-5.

- *Cyber Security Incident that was an attempt to compromise one or more systems identified in the "Applicable Systems" column* - Due to the lower severity of these unsuccessful attempts at compromising ESP(s), EACMS, or BES Cyber System(s), the SDT proposed a longer reporting timeframe. The intent behind the decision to add "By the end of the next calendar day" (11:59 pm local time) was to give responsible entities additional time to gather facts prior to notifications for the less severe attempts to compromise Applicable Systems. It is important to note that compliance timing begins with the entity's determination that attempt to compromise meets the process they defined in Requirement R1 Part 1.2.1.
- The SDT understands initial notification may not have all the details when first submitted. It is expected, however, that information that has been determined is reported within the notification deadlines. Additionally, it is important to note the wording in Requirement R4 Part 4.2. The "compliance clock" for the report timing begins when the Responsible Entity executes its process from Requirement R1 Part 1.2.1 and a determination has been made that the type of incident which has occurred qualifies as reportable.
- Technical rationale taken from the Guidelines and Technical Basis (GTB) CIP-008-5 Requirement 1 provides additional justification for the SDT to maintain the one hour timeframe for Reportable Cyber Security Incidents.
- *"The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."*

In 2007, the Electricity Information Sharing and Analysis Center (E-ISAC) was known as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Its voluntary procedures required the reporting of a cyber-incident within one hour of an incident. CIP-008-1 required entities to report to the ES-ISAC.

In FERC Order No. 706[2] (July 18, 2008), the Commission concluded that the one-hour reporting limit was reasonable [P 663]. The Commission further stated that it was leaving the details to NERC, but it wanted the reporting timeframe to run from the "**discovery**" of the incident by the entity, and not the actual **"occurrence"** of the incident [P 664].

CIP-008-2 and CIP-008-3 were silent regarding the required timeframe for reporting, but it was specifically addressed in CIP-008-5. In the October 26, 2012, redlined version of CIP-008-5, the proposed language for initial notification originally specified "one hour from **identification**" of an incident. This aligned with the Commission's decision in Order No. 706, for the clock to start with the discovery of an incident. However, the Standard Drafting Team changed "one hour from identification" to "one hour from the **determination** of a Reportable Cyber Security Incident". This language was subsequently approved and incorporated into CIP-008-5.

These changes, from "occurrence" to "discovery" to "determination," provide the additional time needed for the entity to apply its specifically created process(es) for determining whether a Cyber Security Incident rises to the level of required reporting. This determination timeframe may include a preliminary investigation of the incident which will provide useful information to other entities to help defend against similar attacks.

---

[2] 2008, Federal Energy Regulatory Commission, Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706.

Notification Updates

Requirement R4 Part 4.3 requires that Responsible Entities submit updates for the required attributes upon determination of new or changed attribute information, if any. The SDT added this language to provide entities sufficient time to determine attribute information, which may be unknown at the time of initial notification, and which may change as more information is gathered. The intent of Requirement R4 Part 4.3 is to provide a method for Responsible Entities to report new information over time as their investigations progress. NOTE: The SDT does not intend updates specified in Requirement R4. Part 4.3 to expose responsible entities to potential violations if, for example, initial and updated notification on the same attribute have different information. This is expected since knowledge of attributes may change as investigations proceed. Rather, the intent of Requirement R4 Part 4.3 is to have a mechanism to report incident information to E-ISAC and NCCIC (and thereby industry) upon determination of each required attribute.

The intent is that the entity report what is known and document the reason not all attributes could become known and ultimately be reported in conditions where, e.g. a Cyber Asset was restored completely, removing all forensic evidence in order to restore operations, which caused the entity to conclude its investigation without having a complete knowledge of the three required attributes.

The SDT asserts that nothing included in the new reporting Requirement R4, precludes the entity from continuing to provide any voluntary sharing they may already be conducting today.

Technical Rationale for Reliability Standard CIP-008-5

This section contains the Guidelines and Technical basis as a “cut and paste” from CIP-008-5 standard to preserve any historical references.

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for Reportable Cyber Security Incidents.

Entities may use an actual response to a Reportable Cyber Security Incident as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise.

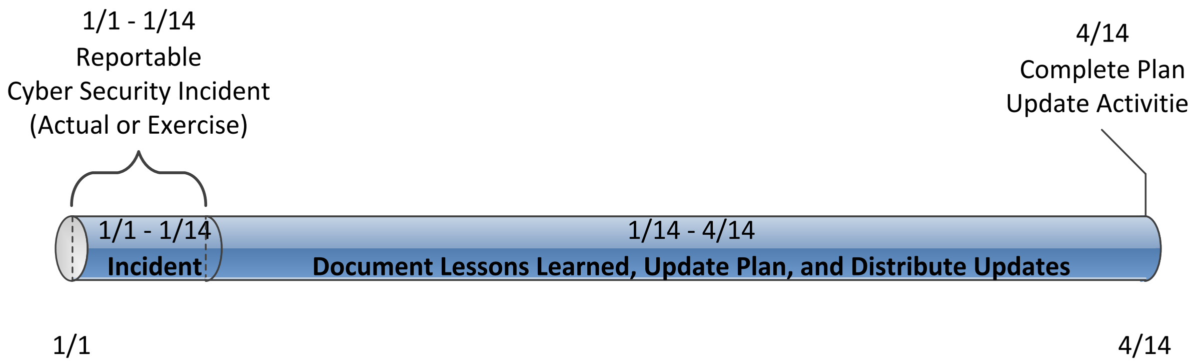
In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for Reportable Cyber Security Incidents. There are several examples of specific types of evidence listed in the measure.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

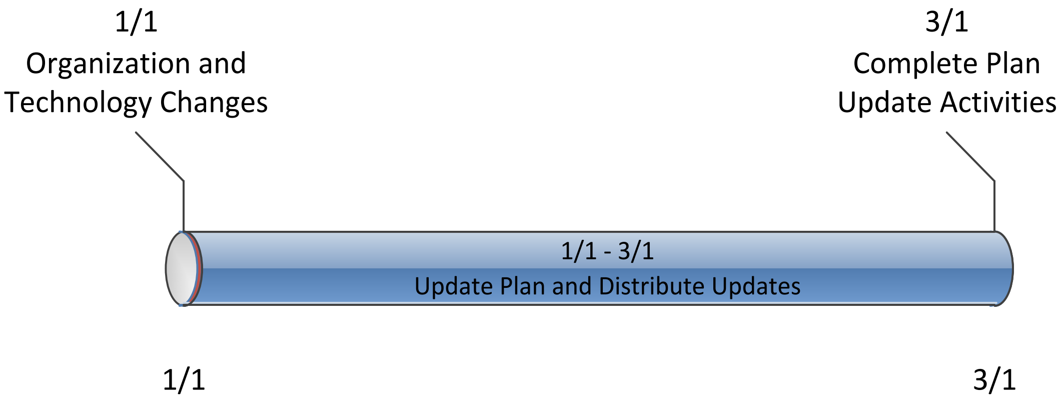
Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents



The activities necessary to complete the lessons learned include updating the plan and distributing those updates.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals.

Figure 2: Timeline for Plan Changes in 3.2



Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)
"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)
Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)
Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)
Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)
Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)
Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)
Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Recovery Plans for BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-009-7

February 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-009-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-009-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-009-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 – Requirement R3

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-009-7 to align recovery planning requirements with the virtualization changes and Shared Cyber Infrastruture (SCI).

The use of the term BES Cyber System has been replaced with "Applicable System" within the requirement language of Requirement R1 Part 1.3 and Requirement R2 Part 2.2 to align the requirement with the applicability for each Requirement Part.

Requirement R1 Part 1.5 has added 'SCI supporting an Applicable System in this Part' to the applicability. This requires that SCI be included in the process to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Having any SCI included in the forensics for a compromised applicable VCA, or the SCI itself, is the reason for the inclusion.

SCI is not specifically included in any other portions of CIP-009. CIP-009 focuses on the ability to recover the BCS functionality, which may or may not require recovery of SCI. The SDT has therefore not included SCI as a direct object of the other recovery plan Requirements and Parts. However, if recovery of the Applicable System's functionality is dependent on recovery of any SCI, then the recovery plan(s) should include such dependencies.

Former Background Section from Reliability Standard CIP-009-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.

An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-009-6

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-009-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event.

Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

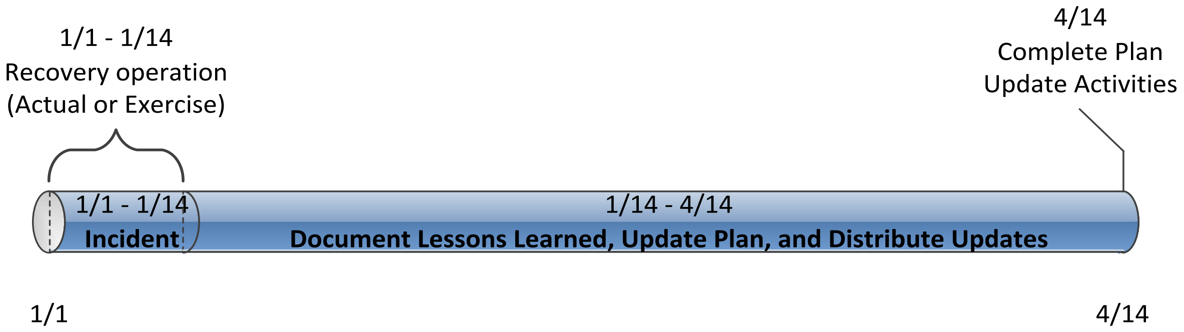


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

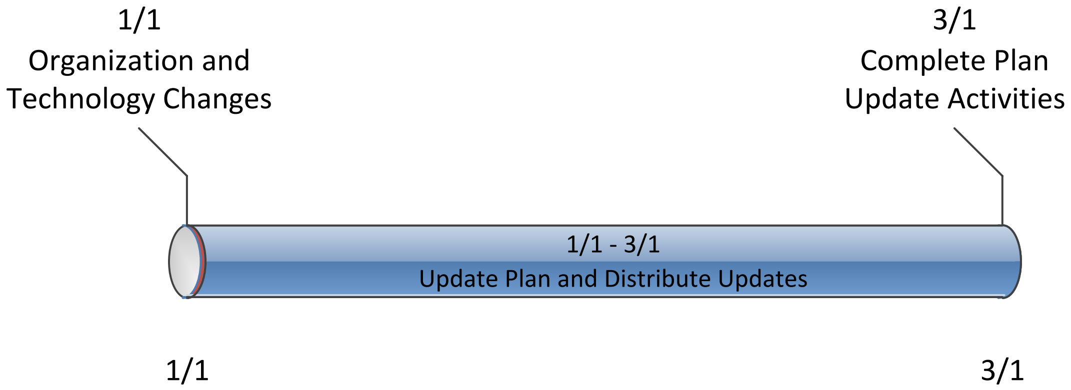


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-5

February 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-010-5

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-5. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-010-5 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

The proposed changes in CIP-010-5 from the Project 2016-02 SDT concern the use of several facets of virtualization technologies. Virtualization allows for such technologies as new controls for Shared Cyber Infrastructure (SCI), remediation VLAN, parent/child images, and dormant virtual machines (VMs). Enabling and clarifying the use of these technologies is the basis of the proposed changes in CIP-010-5. A general introduction to each of these technologies follows.

Shared Cyber Infrastructure (SCI)

Virtualization abstracts the software layers (the OS and applications) from the underlying hardware to allow for hardware to be shared among several Virtual Cyber Assets (VCAs). Hypervisors include security controls to keep these workloads logically isolated from one another and their requirements are within other CIP standards such as CIP-005. However, with any type of shared infrastructure, the need for change management requirements is elevated for those security controls that allow for the 'shared' in SCI. Such controls are added to the change management requirements in CIP-010-5.

Remediation VLAN

Remediation VLAN is a term used to describe a logical network segment in which a computing device can be isolated from other production systems and examined to ensure the integrity and validity of the configuration and software installed on the device before it is permitted to transition to the production network segment.

This examination is policy driven, meaning that the administrator is able to configure what the minimum requirements are for admission to the production network. Examples of this might be minimum operating system patch levels or recent anti-virus definitions.

If during the examination of the computing device, it is found to not comply with the requirements defined in the policy, an administrator may intervene to manually remediate the deficiencies, or the system which was used to examine the device may communicate the deficiencies to the device with instructions on how to remediate itself in an automated fashion. After the remediation actions are taken, the computing device can request to be re-examined and if the requirements dictated by the policy are now met, it will be permitted access to the production network segment.

Parent/Child Images

When a VCA is ‘powered on’, it instantiates (“boots”) from a disk image file. Since the boot ‘disk’ is a file and not physical disk, many individual VCAs can use the same “parent” image as the basis for their own “child” image. Among other things, this allows for patching of an OS to occur to a parent image and the child images then pick up that patched image upon their next instantiation.

Dormant VMs

A VCA that is not instantiated (i.e. not ‘booted up’ and executing) is a dormant VM. It exists not as a traditional cyber asset, but simply as a file. VCA’s can be created for specialized purposes such as to run troubleshooting tools and only be instantiated when needed with long periods of times in between, during which they exist as a file. They are not up and running and on the network where they are managed and patched on a regular basis. However, these can go hand-in-hand with remediation VLANs which would bring them up to date as soon as they do instantiate but before they have access to any other systems.

General Considerations

SCI is mutually exclusive from Cyber Assets (CA) by definition. To enable CIP-010-5 for virtualization, the SDT evaluated the existing Applicable Systems and added SCI that supports an Applicable System in each Part. This approach keeps the SCI applicability parallel to each existing variant of medium impact BCS (i.e. Medium Impact BCS vs. Medium Impact BCS with External Routable Connectivity (ERC) vs. Medium Impact BCS at Control Centers etc.).

Requirement R1

General Considerations for Requirement R1

In prior versions, CIP-010 Requirement R1 has required developing a baseline configuration that consisted of five (5) items (OS, installed and custom software, ports, patches). The baseline configuration was then used in the remainder of Requirement R1 and R2 as the basis of change management including testing. At a high level, the CIP-010-4 Requirement Part 1.1 was to develop a baseline configuration, Requirement R1 Part 1.2 was to authorize and document changes to the items in the baseline configuration, and Requirement R1 Part 1.3 was to update the baseline configuration within a specific timeframe of a change. This tended to focus the requirement on documenting past changes.

In CIP-010-5, as the SDT considered the more policy-based and automated virtualization technologies discussed in the previous section, the SDT determined to change the focus of Requirement R1 towards a security objective of authorizing upcoming changes rather than mandating the maintenance of a baseline configuration. Maintaining baseline configurations remains one possible “how”, but it is no longer the only prescribed “how.” The phrase "baseline configuration" has been removed from CIP-010-5 as a result. The items found in the CIP-010-4 "baseline" are now included in the Measures column within CIP-010-5. This maintains compatibility with current state but allows flexibility for virtualization technologies. This also ensures the focus is not on documenting past changes but the authorization of current or future changes, thus making the requirement forward looking with a clearer security objective.

Rationale for Requirement R1 Part 1.1

Conforming changes to Applicable Systems (see General Considerations above).

The original CIP-010 Requirement R1 Part 1.1 included establishing a baseline configuration for assets that included a set of items that would then be monitored for changes in the remaining parts of Requirement R1. Requirement R1 Part 1.1 is similar to what used to be Requirement 1 Part 1.1 - 1.4, and now serves as the focus of the R1 controls. Requirement R1 Part 1.1 is focused on identifying changes that impact controls found within CIP-005 & CIP-007 (Part 1.1), identifying the impacted security controls prior to change implementation (Part 1.1.1), authorizing those changes (Part 1.1.2), and verifying that the controls are not adversely impacted (Part 1.1.3). While a Responsible Entity can benefit from documenting the configuration or the various elements of the previous "baseline", this is no longer a requirement on its own. Maintaining this documentation is now one possible control to use to ensure changes to those elements are managed as required. Additionally, the SDT added CIP Exceptional Circumstances to Part 1.1.1 because identification of impacted cyber security controls prior to change implementation could impede Responsible Entities' efforts to recover from events or conditions that qualify as CIP Exceptional Circumstances.

Dormant VMs were a challenge with the CIP-010-4 focus on baseline documentation, since the dormant VM is really just a file on disk, and as such cannot impact the BCS until it is instantiated, at which time it must be compliant with the requirement. In many cases dormant VMs are patched to current prior to being added to the "production" network. By focusing the Part 1.1 requirement on change management as opposed to documentation of a current configuration, the challenge is mitigated. The Registered Entity must still know what is current, in order to know what security controls are impacted, but the obligation to keep documentation up to date for a dormant VM is removed.

Rationale for Requirement R1 Part 1.2

Requirement R1 Part 1.2 is where CIP-010-4 Requirement R1 Part 1.5 now lands in CIP-010-5, with minor modifications to Part 1.2.1, and conforming changes to remove the 'baseline configuration' terminology to enable for virtualization.

The SDT chose to remove the reliance on a "Technical Feasibility Exception" in favor of permitting "CIP Exceptional Circumstances" in Pat 1.2.1. The SDT contends testing in a test environment prior to implementing any change in production, and documenting test results may impede Responsible Entities' efforts to recover from events or conditions that qualify as CIP Exceptional Circumstances, and that term still requires an entity to document when that condition occurs with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception (TFE).

Additionally, the SDT chose to add to the phrase "that minimizes differences with the production environment" to eliminate the dependency on baseline configuration.

Rationale for Requirement R1 Part 1.3

Conforming changes to Applicable Systems (see General Considerations above).

Requirement R1 Part 1.3 is where CIP-010-4 Requirement R1 Part 1.6 now lands in CIP-010-5, with minor modifications to Part 1.2.1, and conforming changes to remove the 'baseline configuration' terminology to enable for virtualization. The SDT removed the reliance on the baseline from what used to be Requirement 1 Part 1.6, and instead referred to software (firmware where no independent OS exists) version changes as the trigger for the Requirement Part.

Requirement R2

General Considerations for Requirement R2

Conforming changes to Applicable Systems (see General Considerations above).

The SDT has added the term “unauthorized” into Requirement R2 Part 2.1 to focus it on the risk of unauthorized changes. Many implementations will perform this task by monitoring all changes and looking for unauthorized changes within that population. However, if a way to filter out authorized changes can be implemented, and an entity is able then to have methods to monitor just unauthorized changes the SDT’s intent is that should fulfill the requirement.

Requirement R3

Rationale for Requirement R3 Part 3.1

Conforming changes only to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.2

Conforming changes to Applicable Systems (see General Considerations above).

The SDT chose to remove the reliance on a “Technical Feasibility Exception” in favor of the updated term “per system capability”. The SDT contends that the term still requires an entity to document the limit to the system’s capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

In Requirement R3 Part 3.2.1, conforming changes have been made to remove the baseline configuration dependency. Additionally, the SDT chose to add to the phrase “that minimizes differences with the production environment” to eliminate the dependency on baseline configuration.

Rationale for Requirement R3 Part 3.3

The timing of when to enforce this Requirement Part has been an interesting chicken and egg problem. With the inclusion of the language “Prior to becoming a new Applicable System…” the SDT contends that it has resolved this issue, and established that before the new system has applicability, i.e. it has an impact to the BES, this requirement part must be fulfilled.

The SDT’s intent is for the changes to the Protected Cyber Asset (PCA) definition, and the proposed change mentioned above to the requirement part language, should enable the use of remediation VLANs. The concept of “before connecting to a production environment…” is no longer part if this requirement language.

Conforming changes made to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.4

Conforming changes made only to Applicable Systems (see General Considerations above).

Requirement R4

General Considerations for Requirement R4

The SDT updated Requirement R4 to include associated SCI into the scope of the required plans for Transient Cyber Assets (TCA) and Removable Media. The SDT also updated Attachment 1, such that the scope is clarified once within Requirement R4, and applies throughout Attachment 1.

Former Background Section from Reliability Standard CIP-010-4

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-010-4

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

---

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

---

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and

- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.
With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity’s responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity’s security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rationale for Reliability Standard CIP-010-3

This section contains a “cut and paste” of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset’s baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset’s baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity’s use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to “model” the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.

- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.

- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Information Protection

Technical Rationale and Justification for Reliability Standard CIP-011-4

February 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-011-4

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-011-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-011-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

General Considerations

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-011-4 to align information protection requirements with the virtualization changes.

Requirement R1 and R2

Rationale

To enable CIP-011-4 for virtualization, the SDT added "Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part" within the Applicable Systems column of each of the Parts for Requirement R1 – Requirement R2.

Requirement R2 Part 2.1

Requirement R2 Part 2.1 is an objective level requirement focused on protecting BES Cyber System Information (BCSI) rather than 'Cyber Assets' and 'storage media', and modified to include Requirement R2 Part 2.2. This modification creates necessary flexibility, allowing for cryptographic erasure in scenarios where BCSI cannot be mapped to particular disks within virtualized storage, and where BCSI is stored on SCI employing deduplication. This adjustment is also future-looking to better position CIP-011 for the enablement of cloud type scenarios where the disks are owned and/or managed by a third-party as a service to the entity for its BCSI storage, analysis, or use.

Requirement R2 Part 2.2

Requirement R2 Part 2.2 has been deleted because it was consolidated into Requirement R2 Part 2.1.

Former Background Section from Reliability Standard CIP-011-3

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-011-3

Requirement R1

General Considerations for Requirement R1
None

Rationale for Modifications to Requirement R1:
Requirement R1 still specifies the need to implement one or more documented information protection program(s). The SDT does not intend that this requirement cover publicly available information, such as vendor manuals or information that is deemed to be publicly releasable. Information protection pertains to both digital and hardcopy information.

The SDT clarified the intent of protecting BCSI as opposed to protecting the BES Cyber System(s) and associated applicable systems which may contain BCSI. This was achieved by modifying the parent CIP-011-X R1 requirement language to include "for BES Cyber System Information (BCSI) pertaining to Applicable Systems".

Rationale for Modifications to Requirement R1, Part 1.1
Requirement R1, Part 1.1, is an objective level requirement focused on identifying BES Cyber System Information (BCSI). The intent of the SDT was to simplify the requirement language from CIP-011-2 Part 1.1.

Rationale for Modifications to Requirement R1, Part 1.2
Requirement R1, Part 1.2, is an objective level requirement focused on protecting and securely handling BES Cyber System Information (BCSI) in order to mitigate risks of compromising confidentiality. The reference to different states of information such as "transit" or "storage" or "use" was removed. The intent is to reduce confusion of Responsible Entities attempting to interpret controls specific to different states of information, limiting controls to said states, overlapping controls between states, and reduce confusion from an enforcement perspective. By removing this language, methods to protect BCSI becomes explicitly comprehensive.

Requirement language revisions reflect consistency with other CIP requirements.

Requirement R2

General Considerations for Requirement R2
None

Rationale for Requirement R2:
The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BCSI upon reuse or disposal.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement 2 has remained unchanged. The requirements are focused more on the reuse and disposal of BCS rather than BCSI. While acknowledging that such BCS and other applicable systems may have BCSI residing on them, the original intent of the requirement is broader than addressing BCSI. This is a lifecycle issue concerning the applicable systems. CIP-002 focuses on the beginning of the BCS lifecycle but not an end. The potential end of the applicable systems lifecycle is absent from CIP-011 to reduce confusion with reuse and disposal of BCSI. The 2019 BCSI Access Management project did not include modification of CIP-002 in the scope of the SAR. This concern has been communicated for future evaluation.

Technical Rational for Reliability Standard CIP-011-2

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-011-2 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.
>
> Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.
>
> In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-3

February 2022

RELIABILITY | RESILIENCE | SECURITY

**3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com**

Table of Contents

Technical Rationale for Reliability Standard CIP-013-3

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-3. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-013-3 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-013-3 to align supply chain risk management requirements with the virtualization changes.

To enable CIP-013-3 for virtualization, the SDT added "and Shared Cyber Infrastructure (SCI)" to the parent Requirement R1. Additionally, the SDT simplified the applicability in Requirement R1 Parts 1.1 and 1.2 by replacing the long list of applicable systems with a reference to the list in the parent Requirement R1 through the use of this language, "applicable systems listed in Requirement R1". Note: Because CIP-013-3 does not contain the "Table" construct with an "Applicable Systems" column, this term is not defined within Section 4 Applicability. Therefore, where used, "applicable systems" is intentionally not capitalized within the requirement language of Requirement R1 Parts 1.1 and 1.2.

Technical Rationale for Reliability Standard CIP-013-2

This section contains a "cut and paste" of the Technical Rationale for CIP-013-2 standard to preserve any historical references.

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

---

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

---

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

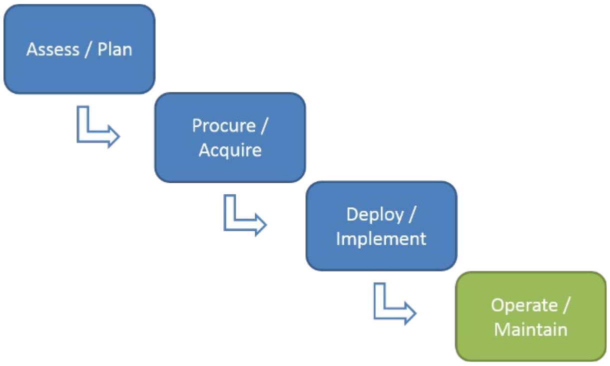
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R3

General Considerations for Requirement R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a “cut and paste” of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

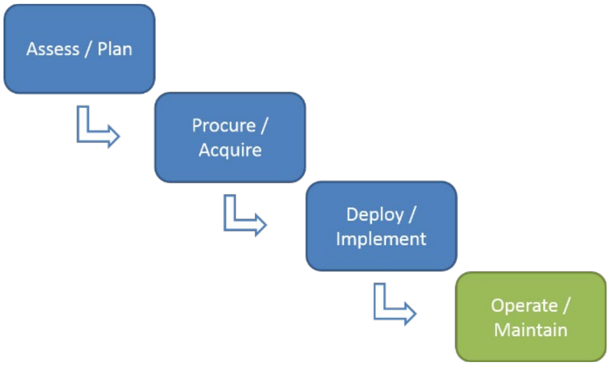
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reminder

Standards Announcement

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Additional Ballots and Non-binding Polls Open through April 11, 2022

Now Available

The additional ballots and associated Violation Risk Factors and Violation Severity Level non-binding polls for the **CIP Virtualization suite of standards (outlined below)** are open through **8 p.m. Eastern, Monday, April 11, 2022**.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-Y - Cyber Security – Security Management Controls
- CIP-004-8 - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-Y - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

Note: Votes cast in the previous ballots, will not carry over to additional ballots. It is the responsibility of the registered voter in the ballot pool to vote again. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

UPDATED

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Formal Comment Period Extended, Now Open through April 11, 2022

Now Available

Due to updated documents on the project page, and to ensure ample time for review, the formal comment period for the **CIP Virtualization suite of standards (outlined below)** has been extended and is now open through **8 p.m. Eastern, Monday, April 11, 2022.**

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-Y - Cyber Security – Security Management Controls
- CIP-004-Y - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-Y - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page**.**

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*

- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 1-11, 2022**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reminder

Standards Announcement

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Additional Ballots and Non-binding Polls Open through April 11, 2022

Now Available

The additional ballots and associated Violation Risk Factors and Violation Severity Level non-binding polls for the **CIP Virtualization suite of standards (outlined below)** are open through **8 p.m. Eastern, Monday, April 11, 2022**.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-Y - Cyber Security – Security Management Controls
- CIP-004-8 - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-Y - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

Note: Votes cast in the previous ballots, will not carry over to additional ballots. It is the responsibility of the registered voter in the ballot pool to vote again. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

UPDATED

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Formal Comment Period Extended, Now Open through April 11, 2022

Now Available

Due to updated documents on the project page, and to ensure ample time for review, the formal comment period for the **CIP Virtualization suite of standards (outlined below)** has been extended and is now open through **8 p.m. Eastern, Monday, April 11, 2022.**

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-Y - Cyber Security – Security Management Controls
- CIP-004-Y - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-Y - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page**.**

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*

- *Please be mindful of ballot and comment period closing dates. We ask to* ***allow at least 48 hours*** *for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts* ***prior to the last day*** *of a comment/ballot period.*

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **April 1-11, 2022**.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/243)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 AB 3 ST
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 247
Total Ballot Pool: 298
Quorum: 82.89
Quorum Established Date: 4/12/2022 2:03:41 PM
Weighted Segment Value: 72.84

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	53	0.791	14	0.209	0	7	11
Segment: 2	8	0.7	1	0.1	6	0.6	0	1	0
Segment: 3	67	1	44	0.88	6	0.12	0	4	13
Segment: 4	15	1	8	0.8	2	0.2	0	2	3
Segment: 5	70	1	40	0.816	9	0.184	0	4	17
Segment: 6	44	1	29	0.829	6	0.171	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	3	0.3	2	0.2	0	2	0
Totals:	298	6.2	178	4.516	45	1.684	0	24	51

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Allen Klassen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Third-Party Comments
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc	John Stickley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Tammy Kubela		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		None	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 298 of 298 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/243)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 3 ST
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 247
Total Ballot Pool: 298
Quorum: 82.89
Quorum Established Date: 4/12/2022 2:05:03 PM
Weighted Segment Value: 73.36

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	54	0.831	11	0.169	0	9	11
Segment: 2	8	0.7	3	0.3	4	0.4	0	1	0
Segment: 3	67	1	41	0.82	9	0.18	0	4	13
Segment: 4	15	1	7	0.7	3	0.3	0	2	3
Segment: 5	70	1	39	0.796	10	0.204	0	4	17
Segment: 6	44	1	29	0.829	6	0.171	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	2	0.2	2	0.2	0	3	0
Totals:	298	6.1	175	4.475	45	1.625	0	27	51

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Allen Klassen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OTP - Otter Tail Power Company	Tammy Kubela		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		None	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 298 of 298 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/243)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 3 ST
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 246
Total Ballot Pool: 296
Quorum: 83.11
Quorum Established Date: 4/12/2022 2:06:17 PM
Weighted Segment Value: 76.97

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	56	0.848	10	0.152	0	8	11
Segment: 2	8	0.7	3	0.3	4	0.4	0	1	0
Segment: 3	67	1	42	0.857	7	0.143	0	5	13
Segment: 4	14	1	7	0.7	3	0.3	0	2	2
Segment: 5	70	1	41	0.837	8	0.163	0	4	17
Segment: 6	43	1	29	0.853	5	0.147	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	296	6.1	181	4.695	38	1.405	0	27	50

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc	Jonathan Robbins		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Tammy Kubela		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Xcel Energy, Inc.	Gerry Huitt		None	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/243)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 3 ST
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 246
Total Ballot Pool: 296
Quorum: 83.11
Quorum Established Date: 4/12/2022 2:08:41 PM
Weighted Segment Value: 60.73

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	41	0.621	25	0.379	0	8	11
Segment: 2	8	0.7	2	0.2	5	0.5	0	1	0
Segment: 3	67	1	36	0.735	13	0.265	0	5	13
Segment: 4	14	1	7	0.7	3	0.3	0	2	2
Segment: 5	70	1	34	0.694	15	0.306	0	4	17
Segment: 6	43	1	23	0.676	11	0.324	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	2	0.2	4	0.4	0	1	0
Totals:	296	6.3	145	3.826	76	2.474	0	25	50

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Comments Submitted
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc	John Stickley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Orlando Utilities Commission	Dania Colon		Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Tammy Kubela		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		None	N/A
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/243)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 AB 3 ST
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 246
Total Ballot Pool: 296
Quorum: 83.11
Quorum Established Date: 4/12/2022 2:13:49 PM
Weighted Segment Value: 76.08

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	53	0.803	13	0.197	0	8	11
Segment: 2	8	0.7	2	0.2	5	0.5	0	1	0
Segment: 3	67	1	42	0.857	7	0.143	0	5	13
Segment: 4	14	1	8	0.8	2	0.2	0	2	2
Segment: 5	70	1	42	0.857	7	0.143	0	4	17
Segment: 6	43	1	28	0.824	6	0.176	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	296	6.1	178	4.641	41	1.459	0	27	50

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Comments Submitted
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc	John Stickley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Tammy Kubela		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		None	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/243)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 3 ST
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 246
Total Ballot Pool: 296
Quorum: 83.11
Quorum Established Date: 4/12/2022 2:30:56 PM
Weighted Segment Value: 61.36

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	46	0.697	20	0.303	0	8	11
Segment: 2	8	0.7	0	0	7	0.7	0	1	0
Segment: 3	67	1	37	0.755	12	0.245	0	5	13
Segment: 4	14	1	7	0.7	3	0.3	0	2	2
Segment: 5	70	1	35	0.714	14	0.286	0	4	17
Segment: 6	43	1	23	0.676	11	0.324	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	2	0.2	2	0.2	0	3	0
Totals:	296	6.1	150	3.743	69	2.357	0	27	50

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Comments Submitted
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Third-Party Comments
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Orlando Utilities Commission	Dania Colon		Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Tammy Kubela		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		None	N/A
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/243)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 AB 3 ST
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 246
Total Ballot Pool: 296
Quorum: 83.11
Quorum Established Date: 4/12/2022 2:37:48 PM
Weighted Segment Value: 78.62

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	58	0.879	8	0.121	0	8	11
Segment: 2	8	0.7	3	0.3	4	0.4	0	1	0
Segment: 3	67	1	43	0.878	6	0.122	0	5	13
Segment: 4	14	1	7	0.7	3	0.3	0	2	2
Segment: 5	70	1	42	0.857	7	0.143	0	4	17
Segment: 6	43	1	30	0.882	4	0.118	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	296	6.1	186	4.796	33	1.304	0	27	50

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Abstain	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc	Jonathan Robbins		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Tammy Kubela		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Xcel Energy, Inc.	Gerry Huitt		None	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/243)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 AB 3 ST
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 245
Total Ballot Pool: 296
Quorum: 82.77
Quorum Established Date: 4/12/2022 2:41:04 PM
Weighted Segment Value: 78.37

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	57	0.864	9	0.136	0	7	12
Segment: 2	8	0.7	3	0.3	4	0.4	0	1	0
Segment: 3	67	1	43	0.878	6	0.122	0	5	13
Segment: 4	14	1	7	0.7	3	0.3	0	2	2
Segment: 5	70	1	42	0.857	7	0.143	0	4	17
Segment: 6	43	1	30	0.882	4	0.118	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	296	6.1	185	4.781	34	1.319	0	26	51

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc	Jonathan Robbins		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Tammy Kubela		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Xcel Energy, Inc.	Gerry Huitt		None	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/243)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 3 ST
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 245
Total Ballot Pool: 296
Quorum: 82.77
Quorum Established Date: 4/12/2022 2:42:24 PM
Weighted Segment Value: 56.69

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	39	0.6	26	0.4	0	8	12
Segment: 2	8	0.7	0	0	7	0.7	0	1	0
Segment: 3	67	1	34	0.694	15	0.306	0	5	13
Segment: 4	14	1	8	0.727	3	0.273	0	1	2
Segment: 5	70	1	31	0.633	18	0.367	0	4	17
Segment: 6	43	1	21	0.618	13	0.382	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	3	0.3	3	0.3	0	1	0
Totals:	296	6.3	136	3.571	85	2.729	0	24	51

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Allen Klassen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Comments Submitted
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Third-Party Comments
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Third-Party Comments
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Orlando Utilities Commission	Dania Colon		Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Tammy Kubela		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		None	N/A
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Negative	Comments Submitted
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/243)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 AB 3 ST
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 245
Total Ballot Pool: 296
Quorum: 82.77
Quorum Established Date: 4/12/2022 2:43:39 PM
Weighted Segment Value: 79.04

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	57	0.877	8	0.123	0	8	12
Segment: 2	8	0.7	3	0.3	4	0.4	0	1	0
Segment: 3	67	1	43	0.878	6	0.122	0	5	13
Segment: 4	14	1	8	0.727	3	0.273	0	1	2
Segment: 5	70	1	42	0.857	7	0.143	0	4	17
Segment: 6	43	1	30	0.882	4	0.118	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	296	6.1	186	4.821	33	1.279	0	26	51

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc	Jonathan Robbins		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Tammy Kubela		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Xcel Energy, Inc.	Gerry Huitt		None	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/243)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 AB 3 ST
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 246
Total Ballot Pool: 296
Quorum: 83.11
Quorum Established Date: 4/12/2022 2:45:32 PM
Weighted Segment Value: 78.62

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	58	0.879	8	0.121	0	8	11
Segment: 2	8	0.7	3	0.3	4	0.4	0	1	0
Segment: 3	67	1	43	0.878	6	0.122	0	5	13
Segment: 4	14	1	7	0.7	3	0.3	0	2	2
Segment: 5	70	1	42	0.857	7	0.143	0	4	17
Segment: 6	43	1	30	0.882	4	0.118	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	296	6.1	186	4.796	33	1.304	0	27	50

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Abstain	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Allen Klassen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Third-Party Comments
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		Affirmative	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Third-Party Comments
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		None	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc	Jonathan Robbins		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Negative	Third-Party Comments
5	OTP - Otter Tail Power Company	Tammy Kubela		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Xcel Energy, Inc.	Gerry Huitt		None	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 | Non-binding Poll AB 3 NB
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 272
Quorum: 81.25
Quorum Established Date: 4/12/2022 3:12:43 PM
Weighted Segment Value: 80

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	78	1	38	0.792	10	0.208	16	14
Segment: 2	8	0.4	1	0.1	3	0.3	3	1
Segment: 3	64	1	37	0.881	5	0.119	10	12
Segment: 4	14	0.9	8	0.8	1	0.1	3	2
Segment: 5	61	1	28	0.778	8	0.222	11	14
Segment: 6	39	1	18	0.783	5	0.217	8	8
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	2	0.2	1	0.1	4	0
Totals:	272	5.6	132	4.333	33	1.267	56	51

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Abstain	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 272 of 272 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 | Non-binding Poll AB 3 NB
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 272
Quorum: 81.25
Quorum Established Date: 4/12/2022 3:13:09 PM
Weighted Segment Value: 77.25

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	78	1	38	0.792	10	0.208	16	14
Segment: 2	8	0.5	3	0.3	2	0.2	2	1
Segment: 3	64	1	34	0.81	8	0.19	10	12
Segment: 4	14	0.9	7	0.7	2	0.2	3	2
Segment: 5	61	1	27	0.75	9	0.25	11	14
Segment: 6	39	1	18	0.783	5	0.217	8	8
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	272	5.8	129	4.334	38	1.466	54	51

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Negative	Comments Submitted
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Abstain	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Comments Submitted
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	MEAG Power	Roger Brand		Negative	Comments Submitted
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 272 of 272 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 | Non-binding Poll AB 3 NB
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 272
Quorum: 81.25
Quorum Established Date: 4/12/2022 3:13:30 PM
Weighted Segment Value: 79.64

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	78	1	40	0.8	10	0.2	14	14
Segment: 2	8	0.4	3	0.3	1	0.1	3	1
Segment: 3	64	1	34	0.829	7	0.171	11	12
Segment: 4	14	0.9	7	0.7	2	0.2	3	2
Segment: 5	61	1	28	0.778	8	0.222	11	14
Segment: 6	39	1	18	0.783	5	0.217	8	8
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	3	0.3	1	0.1	3	0
Totals:	272	5.7	133	4.49	34	1.21	54	51

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Negative	Comments Submitted
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Negative	Comments Submitted
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Negative	Comments Submitted
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 272 of 272 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 | Non-binding Poll AB 3 NB
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 272
Quorum: 81.25
Quorum Established Date: 4/12/2022 3:14:04 PM
Weighted Segment Value: 63.41

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	78	1	28	0.571	21	0.429	15	14
Segment: 2	8	0.4	2	0.2	2	0.2	3	1
Segment: 3	64	1	25	0.625	15	0.375	12	12
Segment: 4	14	0.9	7	0.7	2	0.2	3	2
Segment: 5	61	1	25	0.694	11	0.306	11	14
Segment: 6	39	1	15	0.682	7	0.318	9	8
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	272	5.7	104	3.673	60	2.027	57	51

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Negative	Comments Submitted
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Abstain	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Abstain	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 272 of 272 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 | Non-binding Poll AB 3 NB
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 273
Quorum: 80.95
Quorum Established Date: 4/12/2022 3:15:41 PM
Weighted Segment Value: 82.63

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	41	0.82	9	0.18	14	15
Segment: 2	8	0.4	2	0.2	2	0.2	3	1
Segment: 3	64	1	35	0.854	6	0.146	11	12
Segment: 4	14	0.9	8	0.8	1	0.1	3	2
Segment: 5	61	1	30	0.833	6	0.167	11	14
Segment: 6	39	1	19	0.826	4	0.174	8	8
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	3	0.3	1	0.1	3	0
Totals:	273	5.7	138	4.633	29	1.067	54	52

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 273 of 273 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 | Non-binding Poll AB 3 NB
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 273
Quorum: 80.95
Quorum Established Date: 4/12/2022 3:15:59 PM
Weighted Segment Value: 65.06

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	28	0.571	21	0.429	15	15
Segment: 2	8	0.4	0	0	4	0.4	3	1
Segment: 3	64	1	28	0.683	13	0.317	11	12
Segment: 4	14	0.9	7	0.7	2	0.2	3	2
Segment: 5	61	1	27	0.75	9	0.25	11	14
Segment: 6	39	1	16	0.696	7	0.304	8	8
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	273	5.7	108	3.6	58	2.1	55	52

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Negative	Comments Submitted
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 273 of 273 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 | Non-binding Poll AB 3 NB
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 273
Quorum: 80.95
Quorum Established Date: 4/12/2022 3:16:30 PM
Weighted Segment Value: 83.23

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	43	0.86	7	0.14	14	15
Segment: 2	8	0.4	3	0.3	1	0.1	3	1
Segment: 3	64	1	35	0.854	6	0.146	11	12
Segment: 4	14	0.9	7	0.7	2	0.2	3	2
Segment: 5	61	1	29	0.806	7	0.194	11	14
Segment: 6	39	1	19	0.826	4	0.174	8	8
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	3	0.3	1	0.1	3	0
Totals:	273	5.7	139	4.645	28	1.055	54	52

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 273 of 273 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 | Non-binding Poll AB 3 NB
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 273
Quorum: 80.95
Quorum Established Date: 4/12/2022 3:16:56 PM
Weighted Segment Value: 82.63

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	42	0.84	8	0.16	14	15
Segment: 2	8	0.4	3	0.3	1	0.1	3	1
Segment: 3	64	1	35	0.854	6	0.146	11	12
Segment: 4	14	0.9	7	0.7	2	0.2	3	2
Segment: 5	61	1	29	0.806	7	0.194	11	14
Segment: 6	39	1	19	0.826	4	0.174	8	8
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	3	0.3	1	0.1	3	0
Totals:	273	5.7	138	4.625	29	1.075	54	52

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 273 of 273 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 | Non-binding Poll AB 3 NB
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 273
Quorum: 80.95
Quorum Established Date: 4/12/2022 3:17:07 PM
Weighted Segment Value: 66.46

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	29	0.617	18	0.383	17	15
Segment: 2	8	0.4	0	0	4	0.4	3	1
Segment: 3	64	1	30	0.732	11	0.268	11	12
Segment: 4	14	0.9	7	0.7	2	0.2	3	2
Segment: 5	61	1	25	0.694	11	0.306	11	14
Segment: 6	39	1	15	0.652	8	0.348	8	8
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	3	0.3	1	0.1	3	0
Totals:	273	5.7	109	3.695	55	2.005	57	52

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Negative	Comments Submitted
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Negative	Comments Submitted
1	Western Area Power Administration	Sean Erickson	Barry Jones	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Negative	Comments Submitted
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Negative	Comments Submitted
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Showing 1 to 273 of 273 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 | Non-binding Poll AB 3 NB
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 273
Quorum: 80.95
Quorum Established Date: 4/12/2022 3:17:20 PM
Weighted Segment Value: 82.53

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	41	0.837	8	0.163	15	15
Segment: 2	8	0.4	3	0.3	1	0.1	3	1
Segment: 3	64	1	35	0.854	6	0.146	11	12
Segment: 4	14	0.9	7	0.7	2	0.2	3	2
Segment: 5	61	1	29	0.806	7	0.194	11	14
Segment: 6	39	1	19	0.826	4	0.174	8	8
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	3	0.3	1	0.1	3	0
Totals:	273	5.7	137	4.622	29	1.078	55	52

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Negative	Comments Submitted
2	California ISO	Darcy O'Connell		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 273 of 273 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 | Non-binding Poll AB 3 NB
Voting Start Date: 4/1/2022 12:01:00 AM
Voting End Date: 4/12/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 3
Total # Votes: 221
Total Ballot Pool: 273
Quorum: 80.95
Quorum Established Date: 4/12/2022 3:17:30 PM
Weighted Segment Value: 82.42

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	41	0.854	7	0.146	16	15
Segment: 2	8	0.4	3	0.3	1	0.1	3	1
Segment: 3	64	1	34	0.829	7	0.171	11	12
Segment: 4	14	0.9	7	0.7	2	0.2	3	2
Segment: 5	61	1	29	0.806	7	0.194	11	14
Segment: 6	39	1	19	0.826	4	0.174	8	8
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	3	0.3	1	0.1	3	0
Totals:	273	5.7	136	4.615	29	1.085	56	52

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		None	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Affirmative	N/A
1	Entergy	Brian Lindsey		None	N/A
1	Evergy	Allen Klassen		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Nurul Abser		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Kyle Down		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Chris Hofmann		Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Sean Erickson	Barry Jones	Abstain	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Darnez Gresham		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor		Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		None	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza	Denise Sanchez	Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Angelica Valencia		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand		Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	None	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Zack Heim		Affirmative	N/A
3	Seattle City Light	Laurie Hammack		Abstain	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Hao Li	Paul Haase	Abstain	N/A
4	Seminole Electric Cooperative, Inc.	Jonathan Robbins		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	None	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	George Brown		Affirmative	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		None	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Kevin Salsbury		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		None	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Abstain	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Derek Brown		Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	None	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Negative	Comments Submitted
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Tyson Archie		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Lisa Martin		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Abstain	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Evergy	Thomas ROBBEN		Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Tricia Bynum		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	None	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		None	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Abstain	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		None	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 273 of 273 entries

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization - Draft 3
Comment Period Start Date:	2/18/2022
Comment Period End Date:	4/12/2022
Associated Ballots:	2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 AB 3 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 3 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 3 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 3 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 AB 3 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 3 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 AB 3 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 AB 3 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 3 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 AB 3 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 AB 3 ST

There were 85 sets of responses, including comments from approximately 187 different people from approximately 125 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT has redefined Shared Cyber Infrastructure (SCI) such that it now focuses on cyber infrastructure that shares its hardware resources among VCAs of different impact levels only, which then subjects the SCI to additional requirements. Virtualization infrastructure that only hosts VCAs or associated VCAs of the same impact level is no longer SCI and requires no recategorization from current state. The SDT also removed the SCI identification changes from CIP-002. The SDT believes this greatly simplifies SCI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

2. The SDT has reinstated the currently approved ESP definition and appended language to allow for zero trust models. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal. Please also include any comments on the proposed EAP definition in the response to this question.

3. The SDT modified the ERC definition from the "outside the asset containing" reference point in the previous draft back to an ESP reference point. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

4. The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

5. The SDT modified the VCA definition primarily to include the ability to host them on numerous asset types other than SCI. This allows for current state, where entities consider hypervisors as BCA, EACMS, etc. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

6. The SDT modified numerous other glossary terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

7. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

8. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

9. The SDT revised CIP-010 R1 to focus on defining change, authorizing change, and verifying that CIP-005 and CIP-007 related security controls are not affected by changes. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

10. The SDT made other revisions to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

11. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

12. The SDT has revised numerous VSL's for simplification. Do you agree with the proposed changes? If not, please provide the basis for your disagreement.

13. The SDT has revised the Implementation Plan to include the Planned and Unplanned Changes provisions and to allow for early adoption. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

14. Please provide any additional comments for the drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Santee Cooper	Chris Wagner	1,3,5,6		Santee Cooper	Jennifer Richards	Santee Cooper	1,3,5,6	SERC
					LaChelle Brooks	Santee Cooper	1,3,5,6	SERC
					Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Kris Andrews	Santee Cooper	1,3,5,6	SERC
					Wanda Williams	Santee Cooper	1,3,5,6	SERC
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	3,5	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO

					Jamie Monette	Allete - Minnesota Power, Inc.	1	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc.	2	MRO
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					George Brown	Acciona Energy North America	5	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Tricia Bynum	FirstEnergy - FirstEnergy Corporation	6	RF

					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		PUD No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Dana Showalter	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	IS-NE	2	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Michael Del Viscio	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SERC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC

					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
Eversource Energy	Quintin Lee	1		Eversource Group	Quintin Lee	Eversource Energy	1	NPCC
					Christopher McKinnon	Eversource Energy	3	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Helen Lainis	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC

					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Jim Grant	NYISO	2	NPCC
					John Pearson	ISONE	2	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC

					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					John Hastings	National Grid USA	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	MRO,SPP RE,WECC	SPP RTO	Shannon Mickens	Southwest Power Pool Inc.	2	MRO
					Steven Keller	Southwest Power Pool Inc	2	MRO
Western Electricity Coordinating Council	Steven Rueckert	10		WECC Entity Monitoring	Steve Rueckert	WECC	10	WECC
					Phil O'Donnell	WECC	10	WECC
Lower Colorado River Authority	Teresa Krabe	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Associated Electric	Todd Bennett	3		AECI	Michael Bax	Central Electric Power	1	SERC

Cooperative, Inc.						Cooperative (Missouri)		
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The SDT has redefined Shared Cyber Infrastructure (SCI) such that it now focuses on cyber infrastructure that shares its hardware resources among VCAs of different impact levels only, which then subjects the SCI to additional requirements. Virtualization infrastructure that only hosts VCAs or associated VCAs of the same impact level is no longer SCI and requires no recategorization from current state. The SDT also removed the SCI identification changes from CIP-002. The SDT believes this greatly simplifies SCI. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

George Brown - Acciona Energy North America - 5

Answer	No
Document Name	

Comment

Acciona Energy supports Midwest Reliability Organization's (MRO) NERC Standards Review Forum's (NSRF) comments on this question.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Changes to the definitions have not provided clarity necessary. Diagrams that include examples as to how the definition correlates will be necessary if the redefined definition is not further clarified.

Likes 0	

Dislikes 0

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer No

Document Name

Comment

We believe the inclusion of “Cyber Assets” in the second bullet expands the scope of applicability to include non virtual storage resources that are not currently subject to CIP requirements. This increase of in-scope Cyber Assets goes beyond the standards authorization request. We request “Cyber Assets” be deleted from the second bullet.

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer No

Document Name

Comment

Texas RE is concerned with the following statement: “Virtualization infrastructure that only hosts VCAs or associated VCAs of the same impact level is no longer SCI and requires no recategorization from current state” as it assumes industry consensus on how to categorize virtualization infrastructure, where consensus has not been reached.

Texas RE is concerned that the following scenario can still occur: virtualized BCAs or associated virtualized Cyber Assets of the same or associated impact level hosted on virtualization infrastructure where the Registered Entities categorized the virtualization infrastructure as BCAs, EACMS, PCAs, or non-CIP Cyber Assets.

To ensure that virtualization infrastructure that only hosts VCAs or associated VCAs of the same impact level is categorized and protected in a consistent manner, Texas RE recommends clear and concise language on the categorization and impact rating the hosting virtualization infrastructure should have. Specifically, Texas RE recommends virtualization infrastructure inherit the highest impact rating and categorizations of the VCAs that the virtualization infrastructure is hosting. For example, if virtualization infrastructure is hosting two high impact BCS, three PCAs associated with high impact BCS, and an EACMS associated with high impact BCS, then the virtualization infrastructure should be categorized as a high impact BCS. Implementing high watermarking practices could ensure that the virtualization infrastructure is more reliable and secure.

Likes 0

Dislikes 0

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	No
Document Name	

Comment

CHPD believes that the proposed definition for Shared Cyber Infrastructure (SCI) does not meet the SDT's intent and instead increases the complexity of SCI by creating an extra test (does this SCI host multiple impact ratings?) and introducing significant compliance risk, where something as simple as a configuration change in a VCA (adding a new managed system to an EACMS for example) could inadvertently cause a virtual environment to become SCI. Additionally, if a VCA EACMS is associated with both High and Medium impact BCS, does that make its virtual infrastructure SCI?

CHPD suggests revising the definition of SCI to:

SCI - One or more electronic programmable devices, including the software that shares the devices' resources that:

- In a clustered configuration host one or more Virtual Cyber Assets that include one or more BES Cyber Systems or their associated Electronic Access Control Systems or Physical Access Control Systems.
- Provide storage resources required for system functionality of one or more BES Cyber Systems or their associated Electronic Access Control Systems or Physical Access Control Systems.
- SCI does not include the VCAs or Cyber Assets that utilizes its resources. An SCI supporting an EACMS or PACS is associated with the BES Cyber System the EACMS or PACS is associated with.

CHPD is of the opinion thatSCI should be treated like it is an EACMS, except that it is also subject to the respective requirements of CIP-005 R1 and R2. The Applicable Systems column would then read as:

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS;
- PCA; or
- SCI

Likes 0	
Dislikes 0	

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer	No
Document Name	

Comment

We believe the inclusion of “Cyber Assets” in the second bullet expands the scope of applicability to include non virtual storage resources that are not currently subject to CIP requirements. This increase of in-scope Cyber Assets goes beyond the standards authorization request. We request “Cyber Assets” be deleted from the second bullet.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

Reclamation recommends including Management Modules within the SCI definition.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- CIP-002 has always laid a foundation for CIP with an introduction including the term definitions. Consideration incorporating an introduction and clarification of CIP in CIP-002-7 for first time readers. CIP-002-7 should set the stage with a clear picture and foundation for the cyber asset life cycle.
- In CIP-002-7 Attachment 1 BROS needs the support of the definitions for Entity staff to have a complete process view.   Including the definitions, diagrams and potential examples for the CIP is needed. Please introduce the definition and supporting details for the new terms impact cyber assets including function as BCS, BCA, PCA, EACMS, PACS and Form: SCI, MI, VCA, and CS.   The form and function concept are addressed in CIP-005-7 and CIP-007-7 but should be referenced in CIP-002-7.

Proposed Definitions for incorporation in CIP-002-7:

- BES Cyber Asset (BCA)
- BES Cyber System (BCS)
- Cyber Assets (CA)

- Cyber System (CS)
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate System (IS)
- Management Interface (MI)
- Physical Access Control Systems
- (PACS)
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Shared Cyber Infrastructure (SCI)
- Virtual Cyber Asset (VCA)

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	No
Document Name	

Comment

The direction of the drafting team and new definition greatly simplify SCI. Further clarification is required in the definition for storage associated with SCI and for SCI that supports EACMS and PACS. With respect to the first bullet point, it is possible for SCI to exist outside of a clustered configuration, for example a standalone VMware ESXi system that hosts both a Medium Impact and Low Impact BCS. The clustered configuration wording can be removed to ensure this case is captured.

For SCI that hosts EACMS or PACS, the definition does not clearly identify if it would be acceptable to host VCA that are not in scope of NERC CIP compliance rather than being associated with BCS of a lower impact level. The following wording is suggested:

hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS OR BCS of the same impact categorization

With respect to the second bullet point, it does not completely define what is included in providing storage resources. For example, the following scenarios are not addressed:

If storage is implemented using a SAN, are the fibre channel switches included in SCI?

If storage is implemented using Network Attached Storage (NAS), are the network switches included in SCI?

If storage is located at a geographically different location than the Hypervisor, are Cyber Systems associated with communication networks and data communication links exempt from the definition of SCI. For example, for SCI supporting a VCA that is an EACMS, if a fiber connection goes through a DWDM device for multiplexing, is this device considered SCI since it is required for the VCA to function?

The following wording is proposed that limits the definition to the storage device only and leaves other components to be assessed using the existing criteria:

STORES DATA required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS OR BCS of the same impact categorization.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

We believe the inclusion of “Cyber Assets” in the second bullet expands the scope of applicability to include non virtual storage resources that are not currently subject to CIP requirements. This increase of in-scope Cyber Assets goes beyond the standards authorization request. We request “Cyber Assets” be deleted from the second bullet.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	No
Document Name	

Comment

The sea change being attempted in NERC’s CIP definitions makes the success of the vitualization initiative highly dependent on clear communications, making significantly expanded explanations (with examples) appropriate, including clarifying that the new term, “Shared Cyber Infrastructure,” applies to hypervisors and not GO-TO communications systems.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

Since Management Interface pertains to SCI, we request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA? Does the SDT intend that a SCI must have a PSP but not ESP? Does the SDT intend CIP-008 Reportable Cyber Incident include ESP but not PSP?

Request clarification. Does the SDT intend Low Impact to require more evidence (at the asset level) than BES Cyber Systems because of the addition of SCI (CIP-002 vs CIP-003)? SCI may require more granular evidence.

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST believes the definition of “SCI” should not be limited to only hardware-based platforms hosting “mixed trust” virtual Cyber Assets (e.g., CIP and non-CIP, medium and low impact BCS). Proposed additional requirements for SCI, esp. those addressing control of logical access to management interfaces, should in our opinion apply to shared platforms regardless of whether they are hosting only one impact level of BCS and associated systems or supporting a mixed-trust computing environment. Given that the SDT’s proposed changes to CIP-002 through CIP-011 and CIP-013 would require nearly all Responsible Entities, including those with no virtualized environments, to revise most or all of their compliance documents, NST believes the additional effort to “recategorize” existing shared platforms would be acceptably small.

NST opposes the SDT proposal to not compel Responsible Entities to identify and maintain a list of SCI that support BES Cyber Systems. In order to demonstrate compliance with various CIP-003 – CIP-013 requirements for SCI, a Responsible Entity would surely have to demonstrate that all its SCI were accounted for. NST is aware of the fact there is no existing CIP requirement to maintain an inventory of “associated” devices including PCAs, EACMS, and PACS, but doing so was some years ago memorably characterized by a well-known representative of a Regional Entity as an "implied requirement." NST believes an SDT goal should be to avoid adding to the list of "implied requirements."

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Since Management Interface pertains to SCI, we request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA? Does the SDT intend that a SCI must have a PSP but not ESP? Does the SDT intend CIP-008 Reportable Cyber Incident include ESP but not PSP?

Request clarification. Does the SDT intend Low Impact to require more evidence (at the asset level) than BES Cyber Systems because of the addition of SCI (CIP-002 vs CIP-003)? SCI may require more granular evidence.

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Comments: Delete the phrase “Cyber Assets” from the second bullet point in the proposed definition. The inclusion of “Cyber Assets” in the second bullet as worded could expand the scope of applicability to include non virtual storage resources that are not currently subject to CIP requirements.

If a given cyber system implements computational workload sharing, but does not implement clustering, does it have to be categorized as SCI (“In a clustered configuration,…”)?

More clarification is needed with the distinction between a label (applicable system) and a transition process (non-dormant vs. dormant). Some definitions seem to incorporate aspects of both, which may lead to confusion with interpretation of the definition.

Lastly we would urge the use of diagrams to demonstrate concepts associated with the SCI definition and required aspects of the proposed modifications.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Since the Glossary modifications are the foundation to all Standard changes, the SDT and NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.

Introducing Shared Cyber Infrastructure (SCI) increases the number of Requirements and Parts that a Responsible Entity needs to track compared to simply identifying the hypervisor and associated hardware and “high-water marking” them with the highest identified impact rating BCA/VCA and creating a BCS. Attempting to segregate VM guests by their shared memory and CPU, or by using an undefined “clustered configuration,” increases the opportunity for misconfiguration should the underlying hypervisor move a VM Client to the wrong location or cluster member.

According to publications from the Cloud Security Alliance (see ***Best_Practices_for_Mitigating_Risks_Virtual_Environments_April2015_4-1-15_GLM5.pdf***), a risk factor unique to virtual environments is the hypervisor. Hypervisor is the software and/or firmware responsible for hosting and managing VMs. It provides a single point of access into the virtual environment and is also potentially a single point of failure. A misconfigured hypervisor can result in a single point of compromise of the security of all its hosted components. It does not matter how individual VMs are hardened—a compromised hypervisor can override those controls and provide a convenient single point of unauthorized access to all the VMs. Since all SCI is controlled by the hypervisor, all hypervisors should be high-water marked with any associated level of impact of the VM guests (VCAs) that are identified.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer	No
Document Name	

Comment

SPP appreciates the time and resources the SDT has expended to provide Draft 3 of the virtualization standards. This is not an easy lift. SPP is supportive of the overall approach and structure of the proposed standards. SPP does have concerns with the interpretation of new definitions; and can support with a few clarifications, as described below.

SPP is concerned with how to interpret the definition of Shared Cyber Infrastructure (SCI) and would appreciate clarification by the SDT. First, is clustering included in the definition of SCI. If an entity does not use or implement clustering in its definition, it is still classified as a SCI or would it be a Cyber Asset?

Additionally, of the definition of Virtual Cyber Asset(VCA) describes a “non-dormant logical instance.”   What does the SDT mean by non-dormant in regards to a VCA?   If a virtual machine is not in use, would that be classified as dormant and then once it is needed it becomes a VCA? Would a Golden Image be classified as dormant? Is the term “non-dormant” a permanent state?   To help with interpretation, SPP would appreciate the SDT providing examples of what is meant by “Non-Dormant.”

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	
AWS supports the SCI definition that focuses on cyber infrastructure that shares its hardware resources among VCAs of different impact levels only, which then subjects the SCI to additional requirements to address different cyber security concerns. However, removing SCI from CIP-002 may lead Entities to miss the need to identify, track and apply controls to SCI.	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
IESO supports the comments provided by NPCC and IRC.	
Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	
The use of the term "Cyber Asset" in the 2nd bullet of the SCI definition differs from the intent of a "shared virtual machine" environment. A Cyber Asset is a single programmable electronic device and hence would not reside on a Shared Cyber Infrastructure. *By including the reference to Cyber Asset in this definition could potentially bring additional non virtual storage resources into scope.*	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Since Management Interface pertains to SCI, we request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA? Does the SDT intend that an SCI must have a PSP but not ESP? Does the SDT intend for CIP-008 Reportable Cyber Incident to include ESP but not PSP?

Request clarification. Does the SDT intend Low Impact to require more evidence (at the asset level) than BES Cyber Systems because of the addition of SCI (CIP-002 vs CIP-003)? SCI may require more granular evidence.

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Request clarification of CIP-007, Part 1.3. It appears that applications operating on an SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario, there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, and potentially non-CIP VMs. In the second scenario, there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, and potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support NPCC TFIST's comments. Since Management Interface pertains to SCI, we request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and

from Management Interfaces, and deny all other routable protocol communications, per system capability." This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement? Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA? Does the SDT intend that a SCI must have a PSP but not ESP? Does the SDT intend CIP-008 Reportable Cyber Incident include ESP but not PSP? Request clarification. Does the SDT intend Low Impact to require more evidence (at the asset level) than BES Cyber Systems because of the addition of SCI (CIP-002 vs CIP-003)? SCI may require more granular evidence. Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, "Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability." This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement? Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices. Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Definition of SCI should be consistent regardless of impact rating.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No

Document Name

Comment

We believe the inclusion of “Cyber Assets” in the second bullet expands the scope of applicability to include non virtual storage resources that are not currently subject to CIP requirements. This increase of in-scope Cyber Assets goes beyond the standards authorization request. We request “Cyber Assets” be deleted from the second bullet.

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer No

Document Name

Comment

The SRC agrees with the concept of Shared Cyber Infrastructure (SCI) but does not agree with the proposed wholesale re-write of large parts of existing CIP standards to accommodate the SCI. The proposed changes to existing standards would lead to re-interpretation and change in interpretation of currently effective requirements. This approach also puts a significant operational and financial burden on entities necessitating key program changes and re-investment in CIP tools and protections. The SRC recommends the drafting team consider simpler, lower-impact implementation guidance updates to address SCI which would be applicable to existing CIP requirements.

The SRC notes that the SCI definition seems to incorporate assumptions about the architecture and implementation of virtualization management systems. For this reason, the SRC recommends the use of diagrams within the implementation guidance to demonstrate concepts associated with the SCI definition and required aspects of the applicable standards.

The SRC also notes that further clarification is needed in the following areas which SRC recommends be outlined in the implementation guidance:

- *There is distinction between a label (applicable system) and a transition process (non-dormant vs. dormant). However, SRC notes that some definitions seem to incorporate aspects of both, which may lead to confusion with interpretation of the definition.*

When a cyber-system implements computational workload sharing but does not implement clustering guidance to help the entities determine whether the system meets the categorization of SCI (e.g., “In a clustered configuration,…”).

Likes 0

Dislikes 0

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer No

Document Name

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

Likes 0

Dislikes 0

Response

Joni Jones - Wabash Valley Power Association - 1

Answer	Yes
Document Name	

Comment

Acceptable but convoluted definition. However, does this effectively pull in the current implementation of software defined networking?

Likes 0

Dislikes 0

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP would like more clarification on the SCI definition and how it relates CIP-007 R1.3, this seems like a contradiction.

Likes 0

Dislikes 0

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the redefined Share Cyber Infrastructure (SCI) definition.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer	Yes
Document Name	

Comment

We agree that the new Shared Cyber Infrastructure definition is much clearer.

Likes 0

Dislikes 0

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) agrees with the proposed SCI definition.

Likes 0

Dislikes 0

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Although we agree with the proposed change, it is not explicitly clear that a hypervisor environment hosting VCAs must be categorized as a BCA, EACMS, etc. To avoid confusion the definition for SCI could state that a hypervisor environment hosting virtual cyber assets of the same classification must be categorized as the same type of cyber asset	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the proposed changes made to the definition of SCI.	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Patty Ireland on behalf of DTE Energy, Segments 3 and 4	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the proposed changes to the SCI definition.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes made to the definition of SCI noting the language has been streamlined.	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
SMUD agrees with these changes.	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
We feel the definition greatly simplifies applicable SCI, but we feel prior to the implementation, the concepts associated with the SCI definition and other aspects of the proposed modifications be illustrated to aid in meeting strict compliance. Obviously the modifications have been a moving target, so implementation guidance is on the back burner. Compliance guidance is necessary before the implementation plan starts.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We support NPCC RSC's comments.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	

Kimberly Turco - Constellation - 6

Answer	Yes
Document Name	

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Alison Mackellar - Constellation - 5

Answer	Yes
Document Name	

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

See EEI comment.

Likes 0	

Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments below. ACES Comments: We feel the definition greatly simplifies applicable SCI, but we feel prior to the implementation, the concepts associated with the SCI definition and other aspects of the proposed modifications be illustrated to aid in meeting strict compliance. Obviously the modifications have been a moving target, so implementation guidance is on the back burner. Compliance guidance is necessary before the implementation plan starts.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	2016-02_CIP_Virtualization_DRAFT_3 Unofficial_Comment_Form_02182022-WAPA.docx
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports the comments previously filed by the MRO NSRF and EEI.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	

Exelon will align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon will align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

2. The SDT has reinstated the currently approved ESP definition and appended language to allow for zero trust models. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal. Please also include any comments on the proposed EAP definition in the response to this question.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer	No
Document Name	

Comment

The SRC agrees with the reinstatement of currently approved ESP definition but notes that the EAP definition appears to focus on control of traffic to/from a single BCS and recommends the definition to state “one or more BCS” instead of “a BCS.” The SRC also recommends that host-based firewalls not be considered in scope of the EAP definition. Additionally, the SRC recommends further clarification be provided regarding EAP definition in the following areas:

- *Does the EAP apply to host-based firewalls?*
- *Would each host firewall be a single EAP?*
- *Could an entity identify all such host-based firewalls as an EAP in a group?*

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer	No
Document Name	

Comment

SPP would like the clarification whether the EAP definition applies to host-based firewalls? Would each host firewall be a single EAP? Could an entity identify all such host-based firewalls as an EAP in a group?

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment	
Zero trust does not appear to be included in the revised definition. Please provide more clarification for the added language and its application to zero trust.	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
The new Electronic Security Perimeter (ESP) definition further complicates the situation with respect to mixed-trust environments where a Responsible Entity may choose to create ESPs (Electronic Access Points) for a single Cyber Asset (zero trust paradigm). While this may be easier with standalone physical Cyber Assets – introducing SCI, VCA, virtual clusters, and virtual networking creates complexity that could allow unauthorized access if not carefully configured via the virtual networking, firewall, and policies required to segregate VM guests. Virtual environments still require hypervisor overview for controlling VM guests as well as implementing policies for sizing, network access, and complete lifecycle of the VM guest. Removal of the ESP not only creates a more complex environment by randomly determining where CIP BCS resides within the corporation, it removes the concept of defense-in-depth that is afforded by limiting outside access into these identified BCS through a limited number of points on the ESP. Marrying both ESP and zero-trust within an overall ESP would better serve our Responsible Entities and create a more secure environment as zero-trust Cyber Assets would not be internet-facing while simplifying the management of the environment. Maintaining the ESP, and fully incorporating virtualization and zero trust paradigms within an identified ESP allows Responsible Entities to leverage another layer of defense for BCS by limiting ingress/egress points and access to these Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes the proposed new part of the current ESP definition, “or a logical boundary defined by one or more EAPs” is redundant and unnecessary. We therefore recommend maintaining the currently approved ESP definition. NST believes the proposed definition of EAP (“An electronic policy enforcement point or a Cyber Asset interface that controls routable communication to	

and from a BES Cyber System") is problematic in two respects. First, we believe it could be interpreted to mean an EAP should control all routable communication between a BCS and another Cyber Asset, regardless of whether that device is within or outside of an ESP protecting the BCS. Second, by saying an EAP can be "a Cyber Asset interface" without qualification, the definition could be interpreted to allow for the use of host-based firewalls on BES Cyber Assets and BES Cyber Systems, something the previous set of proposed modifications to CIP-005 expressly prohibited for CIP-005. NST suggests making only minor changes to the well-understood existing definition of EAP, such as: "An electronic policy enforcement point or a Cyber Asset interface on an Electronic Security Perimeter that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter."

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

This definition is very broad and could be considered to include every interface on every asset inside the ESP as well (even in a non-zero trust model) which is used to communicate with each other. This would complicate maintaining the "ESP". The language around communications between assets outside the ESP to assets inside the ESP, and vice-versa, needs to be kept.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP does not support the proposed changes made to the definition of ESP. The SDT added "*; or a logical boundary defined by one of more EAPs*" to the definition of ESP. With this addition, ESP now exclusively requires the use of EAPs and conflicts with the measures in CIP-005-7 R1.2 where an EAP is one of many options to restrict inbound and outbound communications. AEP recommend reverting to the existing ESP definition.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	No
Document Name	

Comment

The definition of ESP is overly redundant and is not cohesive with the definition of EAP. It does not seem necessary to state that ESPs can be a border defined by EAPs, as that this is already handled by the definition of EAP. It also fails to include PCAs in the definition, which is now required given that VCAs that share CPU/memory with a BCA become PCAs even if they do not share network space, and it does not establish ESPs for non-routable devices, which is now needed with the new IRA protections. CHPD suggests revising the definition of ESP and EAP to:

ESP - A logical boundary surrounding one or more BES Cyber Systems or Protected Cyber Assets.

EAP - An electronic policy enforcement point or Cyber Asset interface that controls routable communication through the ESP.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Texas RE agrees with the proposed definition of ESP.

Texas RE recommends the EAP definition be revised to include “or PCA” after “from a BES Cyber System”. The definition as currently written states that the EAP controls routable communication to and from a BES Cyber System. PCAs are also required to be protected by an ESP, however if a PCA is directly connected to a firewall then that interface would not be considered an EAP, as it does not control routable communication to and from a BCS.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes

Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We support NPCC RSC's comments. Additionally, the definition of EAP may be interpreted to include Cyber Assets that convert routable communicatoin to non-routable. Would the port on a serial to IP converter (that meets the CA defintion) meet the definition of EAP? If it does than a BCA that is communicating serial to the converter could be ouside of the ESP. The serial to IP converter would be an EACMS? Would the serial or TCP/IP ports on a RTU that communicates to BCAs (protection system relays) using a routable protocol but to the outside word using a non-routable protocol be an EAP and make the RTU an EACMS? If the TCP/IP ports are are EAPs than the RTU is outside the ESP	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the reinstatement of ESPs and agrees with the change made to allow zero trust models.	
Likes 0	
Dislikes 0	
Response	

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
We support the NPCC TFIST comments. We support the ESP and EAP modifications.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We support the ESP and EAP modifications.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
IESO supports the comments provided by NPCC and IRC	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	Yes
Document Name	
Comment	
Southern supports the reinstatement of ESPs and the appended language to allow for zero trust models.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
AWS supports the SDT’s proposal to reinstate the currently approved ESP definition and appended language to allow for zero trust models. The language allows Entities to adopt a defense-in-depth approach that leverages both traditional perimeter-based security and zero-trust concepts. AWS suggests that the SDT develops detailed implementation guidance that supports traditional perimeter-based security, zero-trust and hybrid approaches, including defining the term zero-trust and/or directing Entities to reference NIST Special Publication 800-207 on the topic for additional clarity.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
We support the ESP and EAP modifications	
Likes 0	
Dislikes 0	
Response	

patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Patty Ireland on behalf of DTE Energy, Segments 3 and 4	
Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
We support the ESP and EAP modifications.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE agrees with the proposed ESP definition.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes

Document Name	
Comment	
We agree with the proposed changes to the ESP definition.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes/reinstatement of the ESP and EAP definitions.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Please include the applicable definitions in CIP-002-7, CIP-005-7, CIP-007-7, and CIP-010-5 for orientation especially for those new to NERC CIP.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Returning to the orginial ESP definition resolves the concerns that BPA previously had with the definition change.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Joni Jones - Wabash Valley Power Association - 1	
Answer	Yes
Document Name	
Comment	
Need to ensure an extremely clear understanding by the industry for the revised definitions of ESP and EAP to ensure that the level of security is not reduced. This will require a common understanding across both industry and auditors for effective implementation that will not be easy to achieve. Further, by allowing the each individual end device to be the logical access point, the language essentially allows an entity to compliantly just run a well configured copy of Windows Firewall as their only EAP control. Not sure if that is the intent.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Scott Kinney - Avista - Avista Corporation - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	

Exelon will align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

3. The SDT modified the ERC definition from the "outside the asset containing" reference point in the previous draft back to an ESP reference point. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Joni Jones - Wabash Valley Power Association - 1

Answer	No
Document Name	

Comment

Language needs to say EAP, not ESP. An EAP is the policy enforcement point or interface, not the ESP.

Likes 0	
Dislikes 0	

Response

Mike Marshall - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

Idaho Power believes the previous definition provided more clarity.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP does not support the proposed changes made to the definition of External Routable Connectivity (ERC) and recommends that ERC should maintain its existing definition. AEP further recommends the SDT to create a new term to address the need for the zero-trust model. The word "External" in "External Routable Connectivity" is defined in the existing definition as "outside of its associated ESP", while the proposed definition of ERC uses "**through** its ESP".

Likes 0	
Dislikes 0	

Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes the use of the word, "through (an ESP)" has the potential to cause confusion over what kind of routable communications qualify as ERC. ERC to or from a Cyber Asset should be clearly defined as "through" an ESP boundary or access point, not "through" an ESP (the online Merriam Webster dictionary defines "through" as "a function word to indicate movement into at one side or point and out at another and especially the opposite side of // 'drove a nail through the board'"). NST believes the existing definition of ERC can and should be retained as-is.	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Removing “outside the asset containing” and identifying the ESP as the boundary where electronic access is required is welcomed. However, specifically identifying EAPs as an ESP in the new definition could potentially create confusion. Further, with no NERC definition for “electronic policy enforcement point” there may be a question as to what constitutes this “enforcement point.” In addition, the “logical boundary defined by one or more EAPs” may inadvertently allow access if an EAP was not correctly identified and configured. Since zero trust is a strategic approach and there is no formal definition, Responsible Entities can create their own definition of what zero trust represents, which creates potential monitoring issues and would require additional Practice and Implementation Guides to find common ground. Modification to the ESP definition to include individual BCS (BCA/VCA via a host firewall or other application) would be preferable, as in most cases the ESP must be identified before an EAP can be. In other words, a zero trust Cyber Asset would have both an identified ESP and an associated EAP allowing access to the Cyber Asset.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	

Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	Yes
Document Name	

Comment

Please include the applicable definitions in CIP-002-7, CIP-005-7, CIP-007-7, and CIP-010-5 for orientation especially for those new to NERC CIP

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed modifications to the ERC definition.

Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Yes, this language is much clearer. Now that the ESP definition has been revised, it makes sense to point back to the ESP as a reference point.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE agrees with the proposed ERC definition.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	

Response

patricia ireland - DTE Energy - 4

Answer	Yes
Document Name	

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 1	Orlando Utilities Commission, 5, Colon Dania
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

No comment

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

Comments: We request more clarification regarding whether traffic between ESPs would be included in the category of ERC, as this may impact interpretation of such traffic as involved with IRA.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer	Yes
Document Name	

Comment

SPP agrees with the proposed change of the ERC definition and recommends further clarification be provided to help entities determine if traffic between ESPs would be included in the category of ERC. This may impact interpretation of such traffic as involved with IRA.

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	Yes
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern supports the modified ERC definition back to the ESP reference point.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes

Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
The revised definition is clear and aligns with the current definition of ERC.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We support NPCC RSC's comments.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)	
Answer	Yes
Document Name	
Comment	

The SRC agrees with the proposed change of the ERC definition and recommends further clarification be provided to help entities determine if traffic between ESPs would be included in the category of ERC. This may impact interpretation of such traffic as involved with IRA.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	

Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Josh Johnson - Lincoln Electric System - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	

Likes 0

Dislikes 0

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	

Response

4. The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

Recommend the following definition:

User-initiated access by a person using a Cyber Asset or VCA, not protected by any of the Responsible Entity's Electronic Security Perimeter(s) (ESP) and using a routable protocol To a Cyber System protected by an ESP.

Remove the following language: "That is converted to a non-routable protocol to a Cyber System not protected by an ESP; or To a Management Interface of Shared Cyber Infrastructure."

A management interface on a Shared cyber asset should reside within the registered entities ESP.

Assets that provide Serial conversion to downstream BES Cyber assets do not communicate to those assets using a routable communication protocol and should not be included in the definition of IRA.

In the proposed revised definition of Interactive Remote Access, the existing phrase "that is not an Intermediate System" would be removed. We are concerned that there is a possibility that an Intermediate System would be considered a Cyber Asset or VCA, not protected by any of the Responsible Entity's Electronic Security Perimeters, resulting in a "hall of mirrors" issue under CIP-005 R2.1. Accordingly we recommend either the phrase "that is not an Intermediate System" or the SDT provide clarity on how the proposed definition avoids compliance issues for Intermediate Systems vis-à-vis CIP-005 R2.1.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AEPCO is signing on to ACES comments below. ACES Comments: The updated definition of Interactive Remote Access, removes the existing phrase “that is not an Intermediate System”. There could be an interpretation where an Intermediate System would be considered an Applicable System, not protected by an ESP. Thus the change appears to resulted in a “hall of mirrors”. We are suggesting the SDT provide clarity within the requirement or definition to avoid compliance issues for CIP-005 R2.1.	
Likes 0	
Dislikes 0	
Response	

Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question.	

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer	No
Document Name	

Comment

The SRC does not agree with the proposed modification to the IRA definition. This type of change would require wholesale re-write of large parts of existing CIP standards to accommodate this change. The proposed change to existing standards would lead to re-interpretation and change in interpretation of currently effective requirements. This approach also puts a significant operational and financial burden on entities necessitating key program changes and re-investment in CIP tools and protections. The SRC recommends the drafting team consider simpler, lower-impact implementation guidance updates to address IRA which would be applicable to existing CIP requirements.

Additionally, the SRC believes that the proposed IRA definition change to require source of user-initiated routed traffic to come from outside the ESP may present concerns to entities leveraging EACMS outside ESP's. The SRC recommends that the SDT consider and document within the implementation guidance the use case of a management/monitoring network outside an ESP with EACMS implementations supporting reliability functions from such a network.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	No
Document Name	

Comment

The updated definition of Interactive Remote Access, removes the existing phrase "that is not an Intermediate System". There could be an interpretation where an Intermediate System would be considered an Applicable System, not protected by an ESP. Thus the change appears to resulted in a "hall of mirrors". We are suggesting the SDT provide clarity within the requirement or definition to avoid compliance issues for CIP-005 R2.1.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley

Answer	No
Document Name	

Comment

The proposed definition, specifically the third bullet, makes the MFA and the use of an Intermediate System in requirements in CIP-005 Part 2.1 and 2.3 a little confusing. At the end of the day, it seems as though the SDT is not intending to require MFA and an Intermediate System required for all SCI (only SCI and management interfaces supporting High and Medium Impact BCS and associated PCA) but because bullet #3 doesn’t specify which SCI is being referred to, it could be interpreted that all interactive access to SCI requires the use of an Intermediate System and MFA. Recommend changing the third bullet to read:

“To a Management Interface of Shared Cyber Infrastructure protected by an ESP”

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We do not agree with the removal of “that is not an Intermediate System.” With the current draft, an Intermediate System could be considered a “Cyber Asset or VCA not protected by any of the Responsible Entity’s ESPs.” Thus, an Intermediate System would be required for an Intermediate System.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support NPCC TFIST comments. Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	
The definition for IRA clarifys the routable protocol to serial conversion scenario based on the rationale provided with the definition. *However, the removal of the following original clarifications used in the definitions is concerning:* *"Remote access originates from a Cyber Asset that is not an Intermediate System..."* *"Interactive remote access does not include system-to-system process communications."* *Concerned without these referencable clarifying statements:* *Intermediate Systems could be considered applicable to CIP-005 R2.1. (aligns with NSRF #4 response)* *system to system process communications becomes a question again.*	
Likes 0	
Dislikes 0	

Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
IESO supports the comments provided by NPCC and IRC.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO	
Answer	No
Document Name	
Comment	
SPP is concerned that a wholesale re-write of large parts of the standards may lead to re-interpretation and substantive change in interpretation of requirements which could lead to significant program changes and re-investment in protections. Would the drafting team consider simpler, lower-impact implementation guidance with existing requirements instead? In this case, the change to IRA to require source of user-initiated routed traffic to come from outside the ESP may present concerns to entities leveraging EACMS outside ESP's. Please also consider the use case of a management/monitoring network outside an ESP with EACMS implementations supporting reliability functions from such a network.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	

The proposed langauge is not clear and confuses the issue.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

As written and presented, there is a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication but have not adequately enforced protections to ensure that malicious actors do not use the ports – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to the definition to ensure validity of communications to Applicable Systems. In addition, approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization and approval of SCI terminology and other definitions associated with virtualization. The SDT has not defined whether user-created scripts and programs that can be modified and scheduled to run independently are considered IRA – even though an unauthorized user could modify it to their benefit. Both scripts and programs can be user-initiated, and with no definition of system-to-system communications there is still lingering issues regarding what system-to-system communications is comprised of.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

Should “or” be added to the end of the first bullet to more clearly define the need to continue dropping through the bullets like a decision tree to identify if any of the points are true instead of exiting after the first question?

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	
Comment	
Comments: In the proposed revised definition of Interactive Remote Access, the existing phrase “that is not an Intermediate System” would be removed. We are concerned that there is a possibility that an Intermediate System would be considered a Cyber Asset or VCA, not protected by any of the Responsible Entity’s Electronic Security Perimeters, resulting in a “hall of mirrors” issue under CIP-005 R2.1. Accordingly we recommend either the phrase “that is not an Intermediate System” or the SDT provide clarity on how the proposed definition avoids compliance issues for Intermediate Systems vis-à-vis CIP-005 R2.1.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	
Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST sees no reason to change the existing definition's use of "remote access client or other remote access technology." The second part of the proposed definition would, as written, apply to any remote connection using a communications path that included routable to serial conversion, regardless of where that conversion took place (e.g., remote location vs. "local," or "inside the BES asset" location). NST is aware of concerns that using phrases such as "outside the asset" in this context might cause confusion about its relationship to electronic access control requirements for BES assets containing low impact BCS, but we nonetheless recommend using it to avoid overly broad application of "IRA" to communications using both routable and serial connections. Finally, NST believes the second bullet, "...That is converted to a non-routable protocol to a Cyber System not protected by an ESP" should apply only to a BES Cyber System not protected by an ESP.	

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Conversion to non-routable protocol in conjunction with authentication break should be sufficient and the subsequent bullets can be simplified in the IRA definition. Language in the proposed definition is unclear due to the use of "or" in the bullet point "That is converted to a nonroutable protocol to a Cyber System not protected by an ESP; or". The use of "or" indicates a choice of only one of the two options, and choosing both options is not available. BC Hydro recommends clarifying the definition to allow the choice of both options. The text "To a Cyber System protected by an ESP" should reside before the colon, and then add language that includes the additional qualifiers (the two subsequent bullets). BCH requests clarity and pertinent use case examples of the newly defnied term of 'IRA'	
Likes 0	
Dislikes 0	
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
PNMR is concerned about IRA definition bullet point #2. This may get rid of the protocol break where IP to serial for a SCADA port was fine, but a user could initiate a session technically. The definition needs to result in user access not just user initiated. This seems to imply IRA can be between devices “not protected by an esp”. Is that really IRA? Overall, the definition is confusing.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	

Answer	No
Document Name	

Comment

Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

The revised definition of IRA provides more clarity than the earlier version. With that said, AEP does not support the proposed changes made to the definition of IRA because we believe additional clarification Is needed on the new term “Management Interface” which is used in the revised definition of IRA. In addition, AEP recommends adding “*of a BCS*” to the end of the last bullet, so it would read “*To a Management Interface of Shared Cyber Infrastructure* ***of a BCS***.”

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

We do not agree with the removal of “that is not an Intermediate System.” With the current draft, an Intermediate System could be considered a “Cyber Asset or VCA not protected by any of the Responsible Entity’s ESPs.” Thus, an Intermediate System would be required for an Intermediate System.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS would like clarification on the proposed IRA definition, specifically we would like to understand the use cases which the 2nd bullet is intended to cover.	
Likes 0	
Dislikes 0	
Response	

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
• **Interactive Remote Access (IRA) –** Please clarify "user initiated" if it is limited to a person at a screen and keyboard or includes scheduled activities from EACMS outside the ESP into clients, agents or ssh into the ESP to SCI, MI, BCA, PCA, or VCA to run privileged application or command that use a protocol that is consider for "interactive user". • Please include the applicable definitions in CIP-002-7, CIP-005-7, CIP-007-7, and CIP-010-5 for orientation especially for those new to NERC CIP.	
Likes 0	
Dislikes 0	
Response	

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	No
Document Name	
Comment	
We do not agree with the removal of "that is not an Intermediate System." With the current draft, an Intermediate System could be considered a "Cyber Asset or VCA not protected by any of the Responsible Entity's ESPs." Thus, an Intermediate System would be required for an Intermediate System.	
Likes 0	
Dislikes 0	

Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	

CHPD appreciates the SDT’s efforts for the modified definition of IRA. However, the definition remains cumbersome with the extra language needed to support SCI, which does not need to be within an ESP. Additionally, because Active Directory and the multi-factor authentication systems are part of the scheme to restrict access to IRA, they implicitly become Intermediate Systems, which is undesirable. CHPD suggests the following revisions:

IRA - User-initiated interactive access by a person from one Cyber Asset or Virtual Cyber Asset to another.

This makes IRA exist everywhere where any access from one (Virtual) Cyber Asset to another (Virtual) Cyber Asset is IRA. We scope what IRA is to be protected in the requirement, not in the definition.

Intermediate System - One or more Electronic Access Control or Monitoring Systems that are used to perform Interactive Remote Access to another Cyber Asset or Virtual Cyber Asset.

The requirement that the Intermediate System be outside the ESP is below in CIP-005 R2.1;Interactive Remote Access and Intermediate System exist, but there are currently no requirements on them.

CIP-005 R2.1
Applicable Systems:
High Impact BCS and their associated:

- PCA; or
- SCI

Medium Impact BCS and their associated:

- PCA; or
- SCI

Requirement:
Permit IRA, if any, only from:

- A Cyber Asset or Virtual Cyber Asset within a Responsible Entity's ESP
- An Intermediate System outside any ESP

This provides the scope for the requirement to only allow IRA connecting to Applicable Systems from a system protected by the ESP or from the Intermediate System outside the ESP. This also catches serial communications, since IRA is completely agnostic to communication protocol. If a device can connect to a BCA via serial, then it is IRA and that connection is only permitted if the source device is inside the ESP or if it is an Intermediate System.

CIP-005 R2.2
Applicable Systems:

Intermediate Systems used to access Applicable System of Part 2.1

Requirement:

Protect the Confidentiality and Integrity of all IRA connecting to the Intermediate System.

CHPD recommends the following rewording, which puts the verb first.

CIP-005 R2.3

Applicable Systems:

Intermediate Systems used to access Applicable System of Part 2.1

Requirement:

Require multi-factor authentication for all IRA connecting to the Intermediate System.

This is a minor change, as it would technically allow a connection from the Intermediate System to the ESP without MFA if one logs in locally to the Intermediate System. However, this does not seem to be a problem, the Intermediate System is required to be within the Physical Security Perimeter, so it is protected by that layer of protection.

R2.4 through R2.5 can remain as is, as they are not impacted by the suggested change to IRA. R2.6 should be deleted as it is covered by R2.1 now.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

We do not agree with the removal of “that is not an Intermediate System.” With the current draft, an Intermediate System could be considered a “Cyber Asset or VCA not protected by any of the Responsible Entity’s ESPs.” Thus, an Intermediate System would be required for an Intermediate System.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We support NPCC RSC's comments.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed simplified definition of IRA.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the simplified IRA definition.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes

Document Name	
Comment	
Patty Ireland on behalf of DTE Energy, Segments 3 and 4	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	
We agree with the proposed change.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
While the IRA definition is usable, BPA suggests making the following alterations to correct an apparent omission, ensure that scope is clearly limited to BCS, and ensure that grammar is less open to interpretation: User-initiated access by a person using routable protocol and a Cyber Asset or VCA not protected by any of the Responsible Entity's Electronic Security Perimeter(s) (ESP) that is: • To a cyber system protected by an ESP; or • Converted to a non-routable protocol to a BCS not protected by an ESP; or • To a Management Interface of Shared Cyber Infrastructure.	
Likes 0	
Dislikes 0	

Response	
Joni Jones - Wabash Valley Power Association - 1	
Answer	Yes
Document Name	
Comment	
While we agree, one risk with this definition and CIP-005 is that it is ambiguous where a software defined networking management plane would fall into the control environment.	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

5. The SDT modified the VCA definition primarily to include the ability to host them on numerous asset types other than SCI. This allows for current state, where entities consider hypervisors as BCA, EACMS, etc. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.	
Joni Jones - Wabash Valley Power Association - 1	
Answer	No
Document Name	
Comment	
The phrase “excluding logical instances that are being actively remediated” does not accrurately communicate the intent and provides no clear indication what actively remediated means. Further, this provides an incredible amount of ambiguity for enforcement on timing, and understanding of remediation. We agree with the remainder of the definition.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP would like clarification on the last sentence “excluding logical instance that are being actively remediated”.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
This is a very confusing definition. Please add context to "actively remediated".	
Likes 0	
Dislikes 0	

Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
Virtual Cyber Asset (VCA) New Definition –The definition does not address the possibility of containers. Consider adding language “including containers with operating system, firmware or isolated process”.	
Likes 0	
Dislikes 0	
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
“Non-dormant” and “excluding logical instances that are being actively remediated” feel redundand and sumwhat like a double negative. PNMR recommends the following modification. “A logical instance of an operating system or firmware, on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure; excluding logical instances that are being actively remediated or dormant instances.)	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes the proposed definition should more closely resemble the existing definition of "Cyber Asset" or, better still, be eliminated altogether. The existing definition of "Cyber Asset" could be easily "unbound" from "hardware" with this or a similar modification:	

Change from, "Programmable electronic devices, including the hardware, software, and data in those devices" to, "Hardware-based or virtual programmable electronic devices, including the software and data in those devices."

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

- Virtual Cyber Asset

- The scoping of VCA to include only those virtual machines hosted on BCA, EACMS, PACS, PCA, or SCI appears to exclude other virtual machines. This is a noticeable difference from CA, which includes all programmable assets regardless of classification.
    - We think the expectation may be that the underlying hardware would still be a Cyber Asset, which is clear for individual hypervisors, but is not as clear for clusters, which really aren't addressed outside of the SCI definition. If that was the intent, we recommend adding clarity at least to the rationale.
    - An example where this matters would be on a corporate cluster that hosts no BCA, EACMS, PACS, PCA, and therefor is a cluster that is not SCI. Any virtual machine hosted by that cluster would not be considered a VCA. The scoping in CIP-003 R2 Attachment 1, Section 3.1.i does not include non-VCA virtual machines, so controls may not be in place for that communication. Similarly, in CIP-005 R2, the IRA definition does not include virtual machines that are not VCAs, so they may not be required to go through an Intermediate System
    - MRO recommends that the Virtual Cyber Asset definition not be limited to virtual machines hosted on specific classifications of CAs/SCI, but rather include all virtual machines (similar to how CA includes all programmable electronic devices)
- MRO also observed that the VCA and SCI definitions are circular. SCI may be identified by its hosting of VCA, but VCA may identified by being hosted on SCI.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

The language “on a virtual machine” implies that a VCA is separate and distinct than a virtual machine since it resides “on a virtual machine”. Should the language be something like logical instance of an operating system or firmware ***of*** a virtual machine…”? This may lead to confusion of what requirements are necessary for a VCA vs a VM.

What does actively remediated mean? could be worded better than intances being actively remediated….today we have virtual firmware and OS…non-dormant seems to mean an image not started yet. Clarity needed for “on” what does “on” mean. Should it be changed to “of”?	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
While the definition is specific with regards to dormancy, according to publications from the Cloud Security Alliance (see ***Best_Practices_for_Mitigating_Risks_Virtual_Environments_April2015_4-1-15_GLM5.pdf***), many issues need to be identified and secured in a virtualized environment when dealing with dormant VMs. VM sprawl can create uncontrolled proliferation of dormant VMs and can lead to an unmanageable condition of unpatched and unaccounted-for machines. Further, dormant, and offline VMs can deviate so far from a current security baseline that simply powering them on introduces massive security vulnerabilities (this is specifically mentioned in NIST publication ***NIST.SP.800-125Ar1.pdf***). In addition, inadvertent initiation of a dormant VM that is part of an identified BCS within the ESP would be considered at least a PCA by definition of its connection via a routable protocol within a defined ESP. As stated above, a dormant VM may quickly move out of compliance with respect to security patches or updates that could be a security risk via multiple vulnerabilities for all other BCS within the associated ESP. Active remediation as implied in the new definition of VCA allows a “loophole” as there is no reference for what “active remediation” is. Using “Remediation VLANs” introduce new risks as the VCA may still be required to acquire an IP address (DHCP, if it is not hard-coded) and is required to initiate connections to authorize and authenticate itself prior to determining by policy if the Cyber Asset requires remediation. Poorly constructed, managed, and implemented policies to determine a VCA’s remediation status could allow persistent connections of VCA without proper updates until such time that the VCA is isolated with the other remediated support system (patches, updates, malicious code updates, etc.). By this action alone, a compromised system that is initiated could create security issues prior to the “remediation mode” or maintenance mode being invoked. Finally, there is no NERC definition of “Remediation VLAN” or “actively remediated” so there may be ongoing issues associated with differences of interpretation between Responsible Entities and the ERO Enterprise. Use of currently available tools to transfer VM Guests from a test or QA environment would allow complete patching, antivirus, updates, etc. prior to introduction of a dormant or new VM Guest into a production environment and keep the proliferation of dormant VM Guests to a minimum.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The proposed definition is too ambiguous. Please provide more context around “non-dormant”.	

Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO	
Answer	No
Document Name	
Comment	
SPP has concerns for the definition of Virtual Cyber Asset(VCA) describes a "non-dormant logical instance." What does the SDT mean by non-dormant in regards to a VCA? If a virtual machine is not in use, would that be classified as dormant and then once it is needed it becomes a VCA? Would a Golden Image be classified as dormant? Is the term "non-dormant" a permanent state? To help with interpretation, SPP would appreciate the SDT providing examples of what is meant by "Non-Dormant."	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	
As noted by the drafting team in the *Technical Rationale, Project 2016-02 Modifications to CIP Standards New and Modified Terms, and Exemption Language Used in NERC Reliability Standards*, the "one-to-one relationship between a Cyber Asset and its underlying hardware is what virtualization intentionally breaks to increase reliability and resiliency." Breaking the one-to-one relationship introduces new concepts like containerization that have security implications. Applications can be containerized, including critical applications that could pose a direct impact to the grid, just as a physical on-prem BCA. We suggest revising the definition to "…logical instance of an operating system, firmware, or containerized application, on a virtual machine…" Additionally, page 8 of the *Technical Rationale, Project 2016-02 Modifications to CIP Standards New and Modified Terms, and Exemption Language Used in NERC Reliability Standards* that states that "the phrase 'excluding logical instances that are being actively remediated' excludes those that are instantiated but are being remediated in an isolated environment before they are moved to production networks and begin providing their function or service" could be interpreted to mean that test environments or isolated environments are necessary for VCAs regardless of Impact Rating or device classification. The proposed CIP-010-5 R1, Part 1.2 is the only Requirement that discusses test environments, and only requires changes to be tested in a test environment prior to being deployed to production for High Impact BCS.. We suggest clarifying the VCA definition and/or technical rationale to state what is meant by "being actively remediated." Standard Drafting team should clarify their intention by stating whether the term "being actively remediated" is mean to address both the configuration of a new VCA prior to it being moved to a production environment to perform its function, or if the intention spans to change management activities such as patching and configuration	

changes. Implementation guidance for remediating logical instances such as requiring the VCA to be in an environment isolated from production at the time of remediation would also be beneficial.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Non-dormant logical instance needs to be defined, the phrase actively remediated needs to be clarified.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)	
Answer	No
Document Name	
Comment	
The SRC does not agree with the proposed modification to the VCA definition as it does not consider all use cases. The SRC highlights the use case of "active logical instance of an operating system" as a virtual machine running on a Cyber Asset." *Additionally, the SRC requests further clarification be provided regarding the VCA definition in the following areas:* - *exclusion involving remediation and how the how the VCA definition may change during remediation efforts* - *the feasibility and the level of detail required to list all categories of possible applicability as potential hypervisors for a given VCA* *The SRC also notes that there is distinction between a label (applicable system) and a transition process (non-dormant vs. dormant). However, SRC notes that some definitions seem to incorporate aspects of both, which may lead to confusion with interpretation of the definition. The SRC recommends the SDT to modify the term "non-dormant" as follows: If a VM is powered off (dormant), it is not a VCA. Likewise, the tail end of the definition is to prevent an entity from being in violation simply for powering up a VM. As long as that VM is moved to a remediation vlan (like a build network) and remediated it is not a VCA. Once remediated and back into production, it is a VCA again.*	
Likes 0	
Dislikes 0	

Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
The definition is clear and possibly unnecessary given the intent is to simply provide an equivalent virtualized term for a Cyber Asset.	
Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed definition but would like the SDT to provide more clarity on the following:

What does actively remediate mean?

What constitutes dormant vs. non-dormant?

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer	Yes
Document Name	

Comment

We agree with the proposed change.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CEHE agrees with the proposed VCA definition.

Likes 0	
Dislikes 0	

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Although we agree with the proposed change, it is not explicitly clear that a hypervisor environment hosting VCAs must be categorized as a BCA, EACMS, etc. To avoid confusion the definition for SCI could state that a hypervisor environment hosting virtual cyber assets of the same classification must be categorized as the same type of cyber asset	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The direction of the drafting team and new definition address the concern for SCI hosted on multiple classifications of Cyber Assets. The TCA classification was missing. The definition contains a term “Virtual Machine” that is technology specific and does not necessarily apply to all virtualization technologies such as the use of virtualization on a Cisco network switch implementing “Virtual Device Context” (VDC) to run independent instances of the switch on the same hardware. The following is proposed: A non-dormant logical instance of an operating system or firmware, hosted on a BCA, EACMS, PACS, PCA, **TCA** or SCI **THAT SUPPORTS RUNNING MULTIPLE LOGICAL INSTANCES OF AN OPERATING SYSTEM OR FIRMWARE**, excluding logical instances that are being actively remediated	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	

Comment	
AEP supports the definition of new term VCA.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Patty Ireland on behalf of DTE Energy, Segments 3 and 4	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	

No comment

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

Comments: We request clarification on the exclusion involving remediation (“excluding logical instances that are being actively remediated). Does the status of the VCA change during remediation efforts?

What is the distinction between a label (applicable system) and a transition process (non-dormant vs. dormant)? Some definitions seem to incorporate aspects of both, which may lead to confusion with interpretation of the definition.

We believe there needs to be some language somewhere that addresses the phrase “non-dormant” in the definition. While we acknowledge that, at face value, it seems self-explanatory, in practice it’s possible there may be some instances of interpretation. We are not seeking a definition but just some clarity, perhaps in the Technical Guide, that addresses the topic further.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern supports the modified definition of VCA and the ability to host them on numerous asset types other than SCI.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed change.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We support NPCC RSC's comments. Request that guidance be added on the meaning of “remediated” as it is used in the VCA definition and the Technical Guidance and Rationale. Please differentiate between “active remediation” and some other form of remediation.	
Likes 0	
Dislikes 0	
Response	

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	Yes
Document Name	

Comment

ITC supports the comments submitted by EEI

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	Yes
Document Name	

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Alison Mackellar - Constellation - 5

Answer	Yes
Document Name	

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

See EEI comment.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	

Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

6. The SDT modified numerous other glossary terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	No
Document Name	

Comment

While largely in agreement with the proposed changes, we have issues with some of the proposed definitions.

First, we are concerned with the revised definition of Electronic Access Point, specifically with the term “to and from a BES Cyber System.” This could result in every BES Cyber System being considered an EAP, with additional requirements of an EAP. We suggest using second part of the existing definition: An electronic policy enforcement point or a Cyber Asset interface that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Further, the SDT may wish to address how host-based firewalls are treated under the proposed EAP definition (for example, is each host firewall a separate EAP or may be grouped together as one EAP).

Also, we are concerned that the revised definition of Protected Cyber Asset is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states that it is a “Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System…” This description seems to elevate the PCA to the higher watermark level than a BES Cyber Asset, and also seems to fit the definition of SCI. We suggest deleting the second bullet in the proposed PCA definition.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No

Document Name	
Comment	
AEPCO is signing on to ACES comments below. ACES Comments: We agree with most of the modifications to the proposed changes with minor exceptions: Within an ESP in a Zero Trust environment a network can be configured to restrict network traffic via policy enforcement all the way down to the switch port. In this case it is not clear if the policy protecting the BCS is the EAP or is each and every Cyber Asset interface within the Zero Trust environment with an enforcement policy is an EACMS/EAP as each Cyber Asset with a policy pushed from a Zero Trust policy server is an enforment point. This would significantly increase the number of EACMS/EAP within a BCS. We feel there needs to be clarification or exclusions within the definition unless this is the intent of the modifications.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	

Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
For this question, ITC supports the NSRF response	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)	
Answer	No
Document Name	
Comment	
The SRC does not agree with the proposed changes. Specifically, the PCA definition has become significantly more complicated as the current definition is much more straightforward distinguishing only the presence of the PCA network interface(s) in an ESP. Additionally, the SRC believes the mixture of label (applicable system) and process (remediation) does present opportunity for different interpretations of this definition (second bullet).	

Furthermore, the addition of CPU/memory sharing as a criterion for categorizing a Cyber Asset as a PCA does increase the required program coverage of such boundaries as part of CIP-002 process. *SRC requests further clarification be provided regarding the new definition for BCS. In particular, the SRC requests that SDT clarify whether "Acronym only" be revised to include the original language for BCS Or does whether the current proposed redline change indicates that the original text stays and the only change is to the definition term field to include the acronym specifically.*	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
The term Cyber System is not needed since it seems to be only used in CIP-010 R3.3 and IRA definition. The use in the CIP-010 R3.3 requirment is confusing since Cyber System incudes PACS and TCAs and the CIP-010 R3.3 Applicable Systems does not.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
We agree with most of the modifications to the proposed changes with minor exceptions: Within an ESP in a Zero Trust environment a network can be configured to restrict network traffic via policy enforcement all the way down to the switch port. In this case it is not clear if the policy protecting the BCS is the EAP or is each and every Cyber Asset interface within the Zero Trust environment with an enforcement policy is an EACMS/EAP as each Cyber Asset with a policy pushed from a Zero Trust policy server is an enforment point. This would significantly increase the number of EACMS/EAP within a BCS. We feel there needs to be clarification or exclusions within the definition unless this is the intent of the modifications.	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

Electronic Access Point: BHE does not agree with the revised definition of Electronic Access Point, specifically with the term “to and from a BES Cyber System.” This could result in every BES Cyber System being considered an EAP, with additional requirements of an EAP. Suggest using second part of the existing definition: An electronic policy enforcement point or a Cyber Asset interface that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.”

Protected Cyber Asset: BHE does not agree with the revised definition of PCA because it is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states it is a “Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System…” This description seems to elevate the PCA to the higher watermark level of the BCA, and also seems to fit the definition of SCI. Suggest deleting the second bullet in the PCA definition.

Likes 0	
Dislikes 0	
Response	

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	

We support NPCC TFIST comments.

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA?

Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA?

Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	
As written, the new definition for Management Interface is unclear of its intended description. Based on the rationale, it is understood why the need to define these interfaces. However, this definition differs from the virtual machine concept and extends to application functionality tools. Thus bringing additional devices into scope even for those entities that are not using virtual machines. Proposing the 2nd and 3rd bullet are removed from the definition.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
IESO supports the comments provided by NPCC and IRC	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	

Management Interface: The new language attempts to simplify the definition by describing what Lightsout Management (LOM) is in the definition itself but may limit an Entity's ability to clearly identify and appropriately classify all possible management interfaces. LOM is industry accepted terminology and we recommend reverting to the previous iteration of the definition.

Transient Cyber Asset (TCA):

The modification to the Transient Cyber Asset definition that allows virtual machines running on a physical TCA to be treated as software on the device should be reconsidered. As written, an entity may not apply the appropriate security controls to the virtual machines running on physical TCAs. Entities should be monitoring the state of the virtual machines running on their physical hardware for security issues.

We propose removing the language "Virtual machines hosted on a physical TCA can be treated as software on that physical TCA" from the TCA definition. By removing this language, entities would be required to apply security controls to the virtual machines hosted on their physical TCAs in alignment with CIP-010 R4.

Virtual Cyber Asset:

As noted by the drafting team in the *Technical Rationale, Project 2016-02 Modifications to CIP Standards New and Modified Terms, and Exemption Language Used in NERC Reliability Standards*, the "one-to-one relationship between a Cyber Asset and its underlying hardware is what virtualization intentionally breaks to increase reliability and resiliency." Breaking the one-to-one relationship introduces new concepts like containerization that have security implications.

Applications can be containerized, including critical applications that could pose a direct impact to the grid, just as a physical on-prem BCA. We suggest revising the definition to "…logical instance of an operating system, firmware, or containerized application, on a virtual machine…".

Additionally, page 8 of the *Technical Rationale, Project 2016-02 Modifications to CIP Standards New and Modified Terms, and Exemption Language Used in NERC Reliability Standards* that states that "the phrase 'excluding logical instances that are being actively remediated' excludes those that are instantiated but are being remediated in an isolated environment before they are moved to production networks and begin providing their function or service" could be interpreted to mean that test environments or isolated environments are necessary for VCAs regardless of Impact Rating or device classification. The proposed CIP-010-5 R1, Part 1.2 is the only Requirement that discusses test environments, and only requires changes to be tested in a test environment prior to being deployed to production for High Impact BCS..

We suggest clarifying the VCA definition and/or technical rationale to state what is meant by "being actively remediated." Standard Drafting team should clarify their intention by stating whether the term "being actively remediated" is meant to address both the configuration of a new VCA prior to it being moved to a production environment to perform its function, or if the intention spans to change management activities such as patching and configuration changes. Implementation guidance for remediating logical instances such as requiring the VCA to be in an environment isolated from production at the time of remediation would also be beneficial.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer	No
Document Name	

Comment

SPP has the following comments on the proposals for glossary terms.

- SPP is concerned that the SDT has revised the definition of BES Cyber System as an "Acronym Only" while still including the term in the other definitions. SPP recommends the definition be added back to the term or removed from all of the standards where it is still included. "Cyber System" should also reference "BES Cyber System" to show their continuity.
- Intermediate System has been removed from the ESP, thereby lessening the security of an Intermediate System.The PCA definition has become significantly more complicated.
- The previous definition was much more straightforward with the only distinction being presence of the PCA network interface(s) in an ESP.
- The mixture of label (applicable system) and process (remediation) does present opportunity for different interpretations of this definition (second bullet).
- The addition of CPU/memory sharing as a criterion for categorizing a Cyber Asset as a PCA does increase the required program coverage of such boundaries as part of CIP-002 process.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

BES Cyber Asset – Dominion does not agree with the proposed VCA definition.

Cyber System – Dominion found this definition to be confusing. A Cyber System is not defined by being part of the BES. Was the intent behind this to expand Cyber System beyond BES Cyber System? Please clarify.

Electronic Access Point (EAP) – Please provide more clarification on what electronic policy enforcement point means.

Management Interface – Does this definition include all power management devices? For example, does it include UPSs regardless of the access controls on the device?

Protected Cyber Aset (PCA) – Please provide clarity around what is included in "actively remediating prior to introduction to an ESP" (second bullet).

Removable Media – Dominion thinks the examples are necessary and suggests adding examples of virtual removable media.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	
Comment	

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	
Comment	

Comments: We are concerned that the revised definition of Protected Cyber Asset is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states that it is a “Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System…” This description seems to elevate the PCA to the higher watermark level than a BES Cyber Asset, and also seems to fit the definition of SCI. We suggest deleting the second bullet in the proposed PCA definition. Further, the SDT may wish to address how host-based firewalls are treated under the proposed EAP definition (for example, is each host firewall a separate EAP or may be grouped together as one EAP?).

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	
Comment	

Management Interface

- Management Interface

- oIt is still unclear if Management Interface includes software that resides on a different CA from the SCI.

- The first bullet in the definition appears to include vCenter and the third bullet appears that it would include firewall orchestration implementations. Both are typically on a separate CA or virtual machine, rather than being integrated into the hypervisor cluster or firewall appliances.
- MRO is concerned that the only required controls of the Management Interfaces are network access in CIP-005 Part 1.3 (no CIP-004, CIP-007, CIP-010, etc. controls are applicable to Management Interfaces).

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA?

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST considers the statement in the proposed definition of TCA, " Virtual machines hosted on a physical TCA are treated as software on that physical TCA" to be oddly inconsistent with the proposed definition of VCA. Furthermore, we disagree with the SDT's opinion that if a physical TCA hosts multiple virtual TCAs, there should be no need to track and manage each individual physical and virtual device.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

Management Interfaces: Why is it restricted to SCI and EACMS? The new definition excludes most of BC Hydro's BCS.

TCA definition: It includes VCAs, however, VCAs are defined as being hosted on BCAs, EACMS, PACS and SCI. A TCA is by definition not part of any of those and is connected for less than 30 days. The qualifiers for VCAs and VMs being TCAs are unclear. There is an implication that VCA can be a BCS; however, a BCS cannot be a TCA since a TCA is connected for less than 30 days.

PACS: Are VCA and SCI not Cyber Assets already? Is the differentiation necessary? Please clarify and provide some examples or use cases.

PCA: The new definition requires clarification. "Share CPU or memory" needs clarification, as does the exclusion "are being actively remediated prior to introduction to an ESP."

BC Hydro requests additional clarity on the use of the above definitions, with pertinent examples as appropriate.

Likes 0	
Dislikes 0	

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

Answer	No
Document Name	

Comment

In the EACMS definition, “cyber asset” should be replaced with “Cyber System” since a cyber system can be a single asset. Alternatively, it seems that “Cyber System” is used in only one other location. Does the “Cyber System” definition really need to exist?

In the “Reportable BES Cyber Security Incident” definition, the 1st bullet could be removed since it is the definition of a BES Cyber System if that definition remains.

In the “Removable Media” definition, BHP recommends keeping the examples removed which serve to help less technical individuals understand the intent of related requirements.

For the BCSI definition, BHP is OK with the changes. However, BHP would encourage a review of the BCSI definition to make it more objective in the determination of what is or is not BCSI.

For the TCA definition, BHP is concerned that by removing the removable media sectionit could create confusion regarding the classification of removeable media as a TCA.

In the “Cyber Assets” definition, BHP recommends exapanding the exclusion of SCI

In the Intermediate System definition, BHP believes clarification is needed for the removal of “The Intermediate System must not be located inside the Electronic Security Perimeter”.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Request clarification. Does the SDT intend CIP-008 Reportable Cyber Incident to include SCI but not PCA?	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
The sea change being attempted in NERC's CIP definitions makes the success of the vitualization initiative highly dependent on clear communications, making significantly expanded explanations (with examples) appropriate, including clarifying that the new term, "Shared Cyber Infrastructure," applies to hypervisors and not GO-TO communications systems	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP does not support the proposed definitions of the following terms and offers suggestions below: • Electronic Access Point (EAP): The existing definition of EAP describes the access point as "on an ESP". The proposed definition of EAP expands the definition to indicate any Cyber Asset interface that controls routable communication, and not just the one on the ESP interface. This could lead to the expectation of designating multiple inline EAPs (where multiple devices that control routable communication exist in series). AEP recommends adding additional language "*on an Electronic Security Perimeter*" from the existing definition to the proposed definition. As such, the revised definition should read "*An electronic policy enforcement point or a Cyber Asset interface* ***on an Electronic Security Perimeter*** *that controls routable communication to and from a BES Cyber System*." • External Routable Connectivity (ERC) – See response to Question #3 above	

- Electronic Security Perimeter (ESP) – See response to Question #2 above
- Interactive Remote Access (IRA) – See response to Question #4 above
- Intermediate Systems – Upon review of proposed new Requirement 2.6 in CIP-005-8, we believe the new requirement is not clear, and recommend SDT to consider keeping the existing definition and eliminate CIP-005-8 R2.6.
- Management Interface – AEP recommends SDT to further define “touch panel” in its definition. For example, one may consider touch panel as physical hardware such as on/off switches while another person may consider “touch panel” as a fully developed Human Machine Interface in a logical sense.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

Electronic Access Point: NVE does not agree with the revised definition of Electronic Access Point, specifically with the term “to and from a BES Cyber System.” This could result in every BES Cyber System being considered an EAP, with additional requirements of an EAP. Suggest using second part of the existing definition: An electronic policy enforcement point or a Cyber Asset interface that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.”

Protected Cyber Asset: NVE does not agree with the revised definition of PCA because it is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states it is a “Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System…” This description seems to elevate the PCA to the higher watermark level of the BCA, and also seems to fit the definition of SCI. Suggest deleting the second bullet in the PCA definition.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	No
Document Name	

Comment

The modified term Transient Cyber Asset (TCA) is not consistent with the new term VCA. The standards treat a VCA as an independent Cyber Asset in inventory and not as software. The removal of the following statement is suggested“Virtual machines hosted on a physical TCA are treated as software on that physical TCA.”, instead modifying the definition of VCA to also include that TCA may host a VCA.

Likes 0	

Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	No
Document Name	
Comment	
AZPS agrees with a majority of the modified glossary terms, but has questions regarding: TCA Definition - How is a VCA that’s a TCA work? Circular definition, can this be clarified or additional guidance provided in technical guidance?	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
• Please add acronyms to all CIP definitions to aid in documentation alignment. • **Management Interface** (MI) New Definition Configures an Electronic Security Perimeter should also include Electronic Access Points and Access Control Lists. Recommend: “Configures an Electronic Security Perimeter(s), Electronic Access Point(s), Access Control List(s) or configurations for physical and logical networks.” 3. Please add the acronym of (MI) to Management Interface to allow Entities to apply to documentation. Does Management Interface (MI) include a Bluetooth configuration interface by a tablet or smartphone on an SCI that is capable of rebooting the SCI or uploading new Firmware to the SCI that may impact the SCI and/or container VCAs or configurations?	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	No
Document Name	

Comment

Reclamation recommends the Transient Cyber Asset (TCA) definition should include examples of Virtual Cyber Assets that may be considered TCAs.

Likes 0	
Dislikes 0	

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer	No
Document Name	

Comment

Electronic Access Point: BHE does not agree with the revised definition of Electronic Access Point, specifically with the term “to and from a BES Cyber System.” This could result in every BES Cyber System being considered an EAP, with additional requirements of an EAP. Suggest using second part of the existing definition: An electronic policy enforcement point or a Cyber Asset interface that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.”

Protected Cyber Asset: BHE does not agree with the revised definition of PCA because it is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states it is a “Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System…” This description seems to elevate the PCA to the higher watermark level of the BCA, and also seems to fit the definition of SCI. Suggest deleting the second bullet in the PCA definition.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	No
Document Name	

Comment

PCA definition - CHPD firmly believes there still has been no demonstrated risk of hardware-based virtualization attacks that warrant this definition or requirement. CISA's Known Exploited Vulnerabilities Catalog | CISA only lists a single VM escape vulnerability, which was patched before it was disclosed, and is disputed by the vendor as being in the wild. While a number of VM escape techniques have been disclosed, all have been patched and saw no confirmed exploitation in the wild.

Even speculative execution vulnerabilities like Spectre and Meltdown have not seen any confirmed exploitation in the wild and are effectively patched. Future vulnerabilities can be effectively managed by a Responsible Entity's CIP-007 R2 patching program (or mitigated by a mitigation plan if patching is not possible) and CIP-010 R3 Vulnerability Assessment program. This requirement only serves to restrict entities on architectures and to increase the cost of virtualization to make it untenable.

We can also look to NIST 800-125A, Security Recommendations for Server-based Hypervisor Platforms. While VM Process Isolation is considered the first and possibly most important of the baseline functions, preventing VMs from sharing CPU or memory is not listed as any of the security recommendations to secure hypervisor baseline functions.

Looking to the technical aspects, this ‘requirement’ abuses the functionality of DRS (or similar for non-VMware vendors) in ways that were not intended. DRS affinity rules were not intended as a cyber security tool to prevent side channel attacks, but are intended to ensure availability and performance of VMs, as DRS is fundamentally a tool to allocate distributed resources. There are typically three types of rules; VM-to-VM affinity rules which ensure VM stay together for performance reasons, VM-to-VM anti-affinity rules which ensure that VMs stay apart for redundancy reasons incase a host fails, and VM-to-host rules, which ensure that VMs either stay connected to a specific physical resource. Since DRS rulesets were not intended for security, affinity rules do not generally allow you to specify groups of VMs and cannot share CPU with another group of VMs. That means, for example, an EACMS VM would need to have a rule for every VM that it cannot share CPU and memory with it to comply with this requirement. On an infrastructure that hosts both EACMS and non-CIP devices, this could result in hundreds of DRS rules. If a Responsible Entity were to do this, this would create a massive web of affinity rules that would be unmanageable and potentially create a reliability issue in the event of a hardware failure, where critical VMs might not be able to find a suitable host to run on given affinity restrictions.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

Electronic Access Point: BHE does not agree with the revised definition of Electronic Access Point, specifically with the term “to and from a BES Cyber System.” This could result in every BES Cyber System being considered an EAP, with additional requirements of an EAP. Suggest using second part of the existing definition: An electronic policy enforcement point or a Cyber Asset interface that controls routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.”

Protected Cyber Asset: BHE does not agree with the revised definition of PCA because it is contradictory to the new definition of Shared Cyber Infrastructure. The second bullet in the PCA definition states it is a “Cyber Asset or Virtual Cyber Asset that shares CPU or memory with any part of the BES Cyber System…” This description seems to elevate the PCA to the higher watermark level of the BCA, and also seems to fit the definition of SCI. Suggest deleting the second bullet in the PCA definition.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Definitions such as VCA is not clear and confusing.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	No
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Joni Jones - Wabash Valley Power Association - 1	
Answer	No
Document Name	
Comment	

Definition of TCA: In a VDI based environment, it will be common for VCAs to not be connected for 30 consecutive days. Example, A VDI based operator workstation may only be online for one shift. Under the definition, this could be considered by a entity as a TCA not included in a BES Cyber System. Consider the impact of the definition in this environment for both full function operator workstations and read only operator workstations.

Likes 0	
Dislikes 0	

Response

Ryan Strom - Buckeye Power, Inc. - 5

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

PCA – EEI supports the proposed modified glossary terms but asks for clarification regarding the phrase “prior to the introduction to an ESP” with the second bullet. Additionally, we offer suggested bolded minor edits to the balance of the definition:

Are protected by an ESP but are not part of the highest impact BES Cyber System protected by the same ESP; or

A share**d** CPU or memory with**in** any part of the **BCS**, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to an ESP.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment	
Southern agrees with EEI’s suggestion on clarifying the phrase in PCA; “prior to the introduction to an ESP” and their suggested edits to the phrase.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Although we agree with the glossary term changes, there needs to be a seperate ballot for definition changes in the future.	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Patty Ireland on behalf of DTE Energy, Segments 3 and 4	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

CEHE agrees with the proposed definitions.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	
We agree with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
WECC supports the proposed revisons to the terms, but has a question for consideration. In the Protected Cyber Asset definition was it the intent of the SDT to negate the language 'highest rated' in the second bullet of the definition considering it is included in the first bullet of the definition?	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response

Bridget Silvia - Sempra - San Diego Gas and Electric - 3

Answer

Document Name

Comment

SDG&E Supports EEI's Comments on this question.

Likes 0

Dislikes 0

Response

7. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Joni Jones - Wabash Valley Power Association - 1

Answer	No
Document Name	

Comment

In 1.2, The phrase “through and ESP” should be written “through an EAP”. An EAP is the policy enforcement point or interface, not the ESP.

In 2.4. Would a SAN vendor that provides continuing monitoring using data pushed from the SAN with no inbound capability be classified as a vendor remote access session. Industry clarity is needed associated with this requirement

In the applicability section of 2.6, spell out the applicability for the requirement rather than referencing a separate requirement. Language needs to say EAP, not ESP. An EAP is the policy enforcement point or interface, not the ESP.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Please provide the technical guidelines within the standard document. Can NERC provide an example of what an authenticated vendor initiated remote connection is? What is the definition of an authenticated vendor initiated remote connection?

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Definitions such as SCI is not clear and confusing.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

For 2.1, change to: “Permit Interactive Remote Access (IRA) only through an Intermediate System.” (Delete “authorized” and “if any.”) The term “authorized” could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don’t believe was the SDT’s intent. “if any” is not needed.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

The effective language in the currently approved CIP-005-6 R1.3 has been moved to CIP-005 R1.2. In this move the applicability column has removed EAPs for medium/high impact BCS to being directly applicable to high/medium impact BCS with ERC and their associated PCAs. Texas RE recommends this requirement to remain applicable to the EAPs of medium/high impact BCS.

Texas RE is concerned that the Part 1.4 addresses confidentiality, but excludes integrity from the compliance examples provided. Texas RE notes that there are attacks that involve re-writing ciphertext to alter the contents of the encrypted message/file. The attacker will not be able to gain access to the contents of the message/file, however they will have successfully compromised the integrity of the file/message by altering the eventual output once the message/file is decrypted by the intended audience. Encryption does not provide integrity assurance unless it is accompanied by an integrity control, such as GCM (Galois/Counter Mode).

Texas RE understands this to mean that an entity securing communications with AES-256 would be noncompliant with CIP-005 R1.4 and CIP-005 R2.2 as written, as they would have implemented an encryption control but would not have implemented an integrity control.

An entity securing communications with AES-GCM would be compliant, as both encryption and integrity are addressed via AES-GCM. Is this the SDT's intent? Texas RE recommends it could be clearer by adding an example of an integrity control along with the example of encryption as the confidentiality control to clarify that both confidentiality and integrity are necessary CIP-005 compliance elements.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	No
Document Name	

Comment

CHPD agrees with the proposed changes to CIP-005 Requriement R1, however, CHPD does not agree with the proposed changes to Requirement R2 and have identified areas of concern.

Requirement R2.6 as written is not possible to comply with in regards to SCI. SCI are not ESP assets, but R2.6 requires IRA to pass through the ESP. Secondly, often times the hypervisors and management interface will reside on the same network. It is therefore not possible to isolate those devices from each other to prevent IRA from one to another. CHPD recommends removing R2.6in its entirety.

CHPD appreciates the SDT's efforts and believes the SDT is moving in the right direction however additional modifications are needed.   As it is currently proposed, the definition remains cumbersome with the extra language needed to support SCI, which does not need to be within an ESP. Additionally, because Active Directory and the multi-factor authentication systems are part of the scheme to restrict access to IRA, they implicitly become Intermediate Systems, which is undesirable. CHPD suggests the following revisions:

IRA - User-initiated interactive access by a person from one Cyber Asset or Virtual Cyber Asset to another.

This makes IRA exist everywhere where any access from one (Virtual) Cyber Asset to another (Virtual) Cyber Asset is IRA. We scope what IRA is to be protected in the requirement, not in the definition.

Intermediate System - One or more Electronic Access Control or Monitoring Systems that are used to perform Interactive Remote Access to another Cyber Asset or Virtual Cyber Asset.

The requirement that the Intermediate System be outside the ESP is below in CIP-005 R2.1. As stated previously, Interactive Remote Access and Intermediate System exist but there are currently no requirements on them.

CIP-005 R2.1

Applicable Systems:

High Impact BCS and their associated:

- PCA; or
- SCI

Medium Impact BCS and their associated:

- PCA; or

- SCI

Requirement:

Permit IRA, if any, only from:

- A Cyber Asset or Virtual Cyber Asset within a Responsible Entity's ESP;
- SCI; or
- An Intermediate System outside any ESP

This scopes the requirement to only allow IRA connecting to Applicable Systems from a system protected by the ESP or from the Intermediate System outside the ESP. This also catches serial communications, since IRA is completely agnostic to communication protocol. If a device can connect to a BCA via serial, then it is IRA and that connection is only permitted if the source device is inside the ESP or if it is an Intermediate System.

CIP-005 R2.2

Applicable Systems:

Intermediate Systems used to access Applicable System of Part 2.1

Requirement:

Protect the Confidentiality and Integrity of all IRA connecting to the Intermediate System.

CHPD recommends the following rewording, which puts the verb first.

CIP-007 R2.3

Applicable Systems:

Intermediate Systems used to access Applicable System of Part 2.1

Requirement:

Require multi-factor authentication for all IRA connecting to the Intermediate System.

This is a minor change, as it would technically allow a connection from the Intermediate System to the ESP without MFA if one logs in locally to the Intermediate System. However, this does not seem to be a problem, the Intermediate System is required to be within the Physical Security Perimeter, so it is protected by that layer of protection.

CHPD does not have have any comments regarding R2.4 through R2.5 as they are not impacted to the suggested change to IRA. As stated above, R2.6 should be deleted as it is covered by R2.1 now.

Likes 0	
Dislikes 0	

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer	No

Document Name	

Comment

For 2.1, change to: “Permit Interactive Remote Access (IRA) only through an Intermediate System.” (Delete “authorized” and “if any.”) The term “authorized” could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don’t believe was the SDT’s intent. “if any” is not needed.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- NEE Supports NPCC comments:
- Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?
- Request an update to the Requirement for Part 1.4. The first bullet says, “Confidentiality and integrity controls (such as encryption), or.” Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.
- Request an update to the Requirement for Part 2.2. The first bullet says, “For all Interactive Remote Access IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.” Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.
- Request clarification between Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	No

Document Name	

Comment

Manitoba Hydro agrees with the direction of the SDT to leave existing requiremts intact and add additional requirements to support SCI. The addition of a requirement to restrict routable communication access to management interfaces of SCI and EACMS that enforce an ESP is a sound security practice. The standard should leave open the option of creating an out of band management zone so that routable protocol access can be restricted for a group of Cyber Assets instead of requiring this be administered for every single Cyber Asset. This would also remove the per system capability restriction. The following wording is proposed:

Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications OR permit only needed routable protocol communication through a logical border surrounding a network to which only EACMS or SCI are connected and deny all other routable protocol communication.

The scope of applicable systems for part 2.4 and 2.5 is unclear for SCI, it would seem to leave a gap where the requirement is NOT applicable to vendor remote access to SCI located in an ESP if there is no vendor remote access to BCS. Manitoba Hydro suggest the wording match part 2.1

High Impact BCS and their associated:

• PCA

Medium Impact BCS and their associated :

• PCA

SCI supporting an Applicable System in this Part

To limit the scope to system where vendor remote access has been implemented, the following wording is suggested:

Where vendor remote access is implemented, have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer	No
Document Name	

Comment

For 2.1, change to: “Permit Interactive Remote Access (IRA) only through an Intermediate System.” (Delete “authorized” and “if any.”) The term “authorized” could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don’t believe was the SDT’s intent. “if any” is not needed.

Likes 0	

Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
While AEP agrees with most of the proposed revisions in CIP-005-8, the new Requirement R2 Part 2.6 may not be sufficiently clear where it specifies that communications must be **through an ESP** (i.e., "*Routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.*"). AEP recommends SDT to consider keeping the existing definition of "Intermediate Systems" unchanged and eliminating proposed CIP-005-8 R2.6.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, "Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability." This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement? Recommend an update to the Requirement for CIP-005 Part 1.4. The first bullet says, "Confidentiality and integrity controls (such as encryption), or." Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures. Recommend an update to the Requirement for CIP-005 Part 2.2. The first bullet says, "For all Interactive Remote Access IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System." Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures. Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with "permit authorized Interactive Remote Access." Part 2.2 begins with "for all IRA." We suggest they should share the same beginning.	

Likes 0	
Dislikes 0	

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer	No
Document Name	

Comment

Tacoma Power suggests moving the proposed CIP-005-7 R1 Part 1.4 (Super ESP Control) to 1.6 to maintain the current numbering of the Dial-up (CIP-005-7 R1.4) & malicious communication (CIP-005-7 R1.5) controls.
Additionally, Tacoma Power is concerned with the proposed R1 Part 1.4 language and the inclusion of PSPs. By including PSPs, CIP-005 now relies on physical boundaries within what was previously a Standard which required only logical boundaries. Tacoma Power suggests reinstating a modification version of CIP-006 R1 Part 1.10 to exclude the Super ESP concepts, and include only those within CIP-005, referring to more than one geographical location to reflect the language of Exemption 4.2.3.3.

Suggested CIP-006 R1.10 modification:
“Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same geographic location and Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.”

Suggested CIP-005 R1 Part 1.4 (or 1.6 if moved) modification:
“Protect the data traversing communication networks and data communication links used in extending an ESP to one or more geographic locations through the use of confidentiality and integrity controls (such as encryption),
Excluding...”

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

With respect to CIP-005 R1.2 it is not clear on the use of the phrase "through the ESP"? Use of the term "through" could imply a requirement to perform intra-ESP electronic access controls when the intent is to apply electronic access controls to routable protocol network traffic entering and leaving the ESP. Suggest the SDT consider the language used in R1.6 (entering or leaving an ESP). As EAP acts as a policy enforcement point, should the language referene an EAP instead of an ESP here?

BC Hydro requests clarity on the use of the above referenced terms with pertinent examples as appropriate.

Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

NST notes there is no explicit requirement to protect an SCI with an ESP in R1, while it is clearly implied in R2. This inconsistency should be addressed. NST believes the use of the word, "through" in R1.2 is inappropriate and that "through the ESP" should be replaced with "through an ESP boundary or access point" (the online Merriam Webster dictionary defines "through" as "a function word to indicate movement into at one side or point and out at another and especially the opposite side of // 'drove a nail through the board'").

Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	No
Document Name	
Comment	

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Recommend an update to the Requirement for CIP-005 Part 1.4. The first bullet says, “Confidentiality and integrity controls (such as encryption), or.” Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.

Recommend an update to the Requirement for CIP-005 Part 2.2. The first bullet says, “For all Interactive Remote Access IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.” Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.

Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

- Part 1.3 – The inclusion of ‘per system capability’ with no additional mitigations, could allow an Entity to use implementations that inherently allows unneeded routable protocol communication to and from Management Interfaces. Routable protocol controls to Management Interfaces should be the same as required controls to BCS because of the inherent risk of Management Interfaces. An alternate proposal would be to remove the ‘per system capability’ from CIP-005-8 R1.3, which matches the CIP-005-8 R1.2 controls to a BCS.
- Part 1.5 – The applicable systems are high/medium impact BES Cyber Systems with dial-up and their associated PCAs and supporting SCI. The “with dial-up” qualifier is only applied to the BCS. A PCA or SCI with dial-up connectivity would not be applicable if the associated high/medium impact BCS or supported Applicable System does not have dial-up. An alternate proposal could be to update the “with dial-up” qualifier in the applicable systems column to apply to the intended applicable systems.
- Part 1.6 – Including the ‘Internet Protocol’ qualification in the requirement could inhibit malicious communication detection for future technologies and implementations that may not use a traditional firewall and IP routing. In particular with the change from firewalls as the outer perimeter to a zero-trust implementation, there will likely be more configuration points that aren't also acting as routers, so the inherent protection from non-IP protocols offered by the separation of subnets will no longer be there and other protocols could pass. Furthermore the use of the word ‘or’ between ‘entering’ and ‘leaving’ could allow an entity to only have methods for one direction. Also, SCI and Management Interfaces are not included in the applicable systems. The inherent risk of Management Interfaces should require the same protections as the BCS.
- R2 – The replacement of ‘where technically feasible’ with ‘per system capability’ statement could allow implementations that bypass the controls of an IS, encryption, and/or multi-factor authentication without the additional mitigations that are currently required by a TFE.
- Part 2.3 - The changed language now states 'require multi-factor authentication to the Intermediate System'. Does the 'to' indicate that the authentication has to happen at that IS? The language before was scoped to the IRA session, which allowed for that to occur somewhere along the session. The Technical Rationale says this was intentional to define 'where the requirement for multifactor authentication should be applied'.
    - This could make current implementations noncompliant where multi-factor authentication occurs along the session, but not on the Intermediate System.

- Part 2.4, 3.1, 3.2 – The applicability column qualifier, “with vendor remote access”, is only applied against the BCS, but not the associated PCA or supporting SCI. This could allow SCI with vendor remote access no controls if the supporting BCS does not have vendor remote access. An alternate proposal could be to update the “with vendor remote access” qualifier in the applicable systems column to apply to the intended applicable systems.
- Part 2.6 Similar to the comment in Part 1.6, with the potential move from perimeter-based security to zero-trust, the inherent protections against non-routable protocols provided by the firewall may not necessarily be there. Limiting this to routable protocols, leaves potential for non-routable protocols to access BCAs, etc. from the IS unfettered.
- Part 2.6 requires communications between Intermediate System and SCI go through an ESP, however that is not possible (see reasoning below):

    - R1.3 Requires that routable access to SCI Management Interfaces be controlled, but does not require the SCI to be in an ESP. 2.6 requires that access to the SCI from an IS go through an ESP. Definition of ESP, which is dependent upon the definition of EAP – EAP states “controls routable communication to and from a BES Cyber System”. BES Cyber System is one or more BCAs. BCAs by definition exclude SCI. Intermediate Systems cannot be inside and therefore cannot be a BCA. Therefore communication between an Intermediate System and SCI cannot go through an ESP.
- Part 2.6 – The rationale states that an Intermediate System that shares CPU/memory with a BCS would then be a PCA by PCA definition. It then states that R1.1 requires that since it is a PCA that it be protected by an ESP. We understand that the conclusions intended by the drafting team is that the IS could then not be a PCA because of Part 2.6 requiring it to go through an ESP to access BCS. However, in the case of many small ESPs, the IS could be a PCA to one BCS, but only access other BCS by going through an ESP. As long as it doesn’t access the BCS that made it a PCA, it would be compliant. This could allow an IS that is a VCA to be hosted on the same SCI (hypervisor) as a BCA. An alternate proposal could be to update the requirement to include CPU and Memory affinity controls or update the IS definition to include such CPU and Memory affinity controls.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

There is still a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication but have not adequately enforced protections to ensure that malicious actors do not use the ports – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to ensure validity of communications to Applicable Systems.

CIP-005 Requirement R1 Part1.3 to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters, but no minimum level of encryption is required which could result in older less secure methods being used leaving the data at risk.

CIP-005-8 depends upon approved SCI terminology and other definitions associated with virtualization. Approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization.

There is a significant concern is that an entity could implement “logical isolation” using only a host-based firewall on essential systems that are directly connected to the internet. Thus, exposing them to greater risk as compared the requirements in place today.

Further, introducing Shared Cyber Infrastructure (SCI) increases the number of Requirements and Parts that a Responsible Entity needs to track compared to simply identifying the hypervisor and associated hardware and “high-water-marking” them with the highest identified impact rating and creating a BCS. Allowing “mixed-trust” environments within the same SCI (hypervisor) increases the

complexity and management of the environment as the SDT relaxes the “high-water-marking” required to this point (exceptions being EACMS and PACS – but only with the understanding that the hypervisor and associated SCI is protected as an EACMS or PACS).

Finally, there is no NERC definition of “Remediation VLAN” so therefore the Responsible Entity could keep VMs spun up and within the Remediation network for extended periods of time – without the benefit of protections from the other CIP Standards.

Likes 0	

Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO	
Answer	No
Document Name	
Comment	
Is the intent at the actual Management Interface itself for R1.3 for communications to and from or can we have a management network that that all of management interfaces are on and control access that way? Except for the comments regarding the definitions for VCA, SCI, EAP, PCA, and ERC as noted above in Question 1-6, SPP supports the changes the SDT has made to the Requirements for CIP-005.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
IESO supports the comments provided by NPCC and IRC	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	
We have concerns with the SCI, IRA and Management Interface definitions. These terms are used throughout the Standard.	
Likes 0	

Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Recommend an update to the Requirement for CIP-005 Part 1.4. The first bullet says, “Confidentiality and integrity controls (such as encryption), or.” The requirement should be what to accomplish. Measures should be how accomplished. Requirements should be technology agnostic. We recommend moving encryption to these Measures.

Recommend an update to the Requirement for CIP-005 Part 2.2. The first bullet says, “For all Interactive Remote Access IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.” The requirement should be what to accomplish. Measures should be how accomplished. Requirements should be technology agnostic. We recommend moving encryption to these Measures.

Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support NPCC TFIST comments.

Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?

Recommend an update to the Requirement for CIP-005 Part 1.4. The first bullet says, “Confidentiality and integrity controls (such as encryption), or.” Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.

Recommend an update to the Requirement for CIP-005 Part 2.2. The first bullet says, “For all Interactive Remote Access IRA, protect the confidentiality and integrity (e.g., encryption) of communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.” Requirement should what to accomplish. Measures should be how to accomplish. Requirements should be technically agnostic. We recommend moving encryption to these Measures.

Request clarification between CIP-005 Parts 2.1 and 2.2. Part 2.1 begins with “permit authorized Interactive Remote Access.” Part 2.2 begins with “for all IRA.” We suggest they should share the same beginning.

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

For 2.1, change to: “Permit Interactive Remote Access (IRA) only through an Intermediate System.” (Delete “authorized” and “if any.”) The term “authorized” could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don’t believe was the SDT’s intent. “if any” is not needed.

Likes 0	
Dislikes 0	

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer	No
Document Name	

Comment

Tacoma Power suggests moving the proposed CIP-005-7 R1 Part 1.4 (Super ESP Control) to 1.6 to maintain the current numbering of the Dial-up (CIP-005-7 R1.4) & malicious communication (CIP-005-7 R1.5) controls.

Additionally, Tacoma Power is concerned with the proposed R1 Part 1.4 language and the inclusion of PSPs. By including PSPs, CIP-005 now relies on physical boundaries within what was previously a Standard which required only logical boundaries. Tacoma Power suggests reinstating a modification version of CIP-006 R1 Part 1.10 to exclude the Super ESP concepts, and include only those within CIP-005, referring to more than one geographical location to reflect the language of Exemption 4.2.3.3.

Suggested CIP-006 R1.10 modification:

“Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same geographic location and Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.”

Suggested CIP-005 R1 Part 1.4 (or 1.6 if moved) modification:

“Protect the data traversing communication networks and data communication links used in extending an ESP to one or more geographic locations through the use of confidentiality and integrity controls (such as encryption),

Excluding...”

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	No
Document Name	

Comment

New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.

Likes 0	
Dislikes 0	

Response	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	

Comments: New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	

LES agrees with the majority of proposed changes regarding CIP-005 but has concerns with the 'Technical Feasibility' conforming change which is further detailed in the Question 11 response.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the revised proposed changes to the CIP-005 standard.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	
We agree with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE agrees with the proposed revisions in CIP-005.	

Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Patty Ireland on behalf of DTE Energy, Segments 3 and 4	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Comments: For Requirement 2 Part 2.1, change the language to read: “Permit Interactive Remote Access (IRA) only through an Intermediate System.” (Deleting “authorized” and “if any.”) The term “authorized” could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don’t believe was the SDT’s intent. “if any” is not needed.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	

Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the proposed changes to CIP-005.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Request clarification of the combination of 1) the definition of Management Interface and 2) CIP-005 R1 Part 1.3 Requirement. That Requirement says, “Permit only needed routable protocol communications to and from Management Interfaces, and deny all other routable protocol communications, per system capability.” This combination implies new CIP-002 categorizations for assets with SCI and/or Management Interface. If this conclusion is not correct, please explain why this conclusion is incorrect. If this conclusion is correct, should CIP-002 explicitly state this Requirement?	
Likes 0	

Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)	
Answer	Yes
Document Name	
Comment	
The SRC agrees with the proposed changes to CIP-005. In particular, SRC agrees with the proposed change to R1.2 from a security objective but finds the exclusion for time-sensitive Protection System traffic questionable. The SRC entities do not generally work with such systems in scope. Additionally, the SRC agrees with the proposed change to R1.3 from a security perspective and believes that this is good practice to restrict access to such management interfaces. The SRC also appreciates the exclusions to prevent situations of double-jeopardy regarding other standards as referenced in R1.4. Furthermore, the SRC finds no concerns with the proposed changes to the remaining CIP-005 sub requirements and believes that the proposed change to R1.6 is consistent with good practice.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
See EEI comment.	

Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
For Requirement 2 Part 2.1, change the language to read: “Permit Interactive Remote Access (IRA) only through an Intermediate System.” (Deleting “authorized” and “if any.”) The term “authorized” could be interpreted by auditors to mean that authorization evidence just for the IRA is required for each person having IRA, which we don’t believe was the SDT’s intent. “if any” is not needed.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Referencing Part 2.6, if the definition of IRA is changing to potentially include "…that is converted to a non-routable protocol, to a Cyber System not protected by an Electronic Security Perimeter" but the Part 2.6 requirement states that communication between IS and applicable systems must be through an ESP, that complicates this. It's not clear where the ESP would be if the applicable system isn't in an ESP, but where there is routable communication between the IS and the protocol converter. This would potentially lead to some "Creative" network architectures, which provide limited value.	
Likes 0	
Dislikes 0	
Response	

Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Referencing Part 2.6, if the definition of IRA is changing to potentially include "…that is converted to a non-routable protocol, to a Cyber System not protected by an Electronic Security Perimeter" but the Part 2.6 requirement states that communication between IS and applicable systems must be through an ESP, that complicates this. It's not clear where the ESP would be if the applicable system isn't in an ESP, but where there is routable communication between the IS and the protocol converter. This would potentially lead to some "Creative" network architectures, which provide limited value.	
Likes 0	
Dislikes 0	
Response	

8. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer	No
Document Name	

Comment

The SRC does not agree with several of the key proposed changes to CIP-007. In particular, SRC believes the proposed change will necessitate additional requirements to define accessibility in order to determine what controls are necessary and this may lead to disputes in interpretation. In regards to R1.3, The SRC recommends that SDT modify that requirement to read "by mitigating the risk of sharing CPU resources, show how you detect, deter or prevent risk of shared CPU or memory resources." The SRC believes that, as written, this requirement seems too prescriptive. The SRC agrees with the minor proposed changes to the remaining sub-requirements.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley

Answer	No
Document Name	

Comment

SMUD is not sure why requirements for R1.1 changed or why the measures now include the need to document both port and service instead of logical accessible port or service. From a security objective point of view, there is nothing to gain by changing the requirement or measure here, it's only adding a new layer of confusion based on the new requirement language.

It is not clear how the changes being made are needed to support virtualization. SMUD's recommendation is to leave the requirements as they are unless there is a specific need to address a requirement in support of virtualization technology - this does not appear to be the case.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No

Document Name	Affinity Rules - Eversource comments.pdf

Comment

Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

See attached file for the different scenarios mentioned in the narrative.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

"System hardening" may belong in CIP-010, R1.3: Does risk regarding memory sharing need to be mitigated or completely eliminated, do you need a dedicated host per asset clarification? R2.2: Need more clarity on the frequency of evaluation (35 days from the source or 35 days from the last evaluation?). R4 and R5: Will TFEs still apply by removing the technical feasibility language and replacing it with per system capability? Applicable Systems needs to be defined.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support NPCC TFIST comments.

Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification of CIP-007, Part 1.3. It appears that applications operating on an SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario, there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, and potentially non-CIP VMs. In the second scenario, there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, and potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	No
Document Name	

Comment

We have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard. Additionally, the recategorization of R1 from "Ports and Services" to a broader term of "System Hardening"raises potential differences in interpretations during an audit.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

IESO supports the comments provided by NPCC and IRC

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer	No
Document Name	

Comment

SPP requests that guidance is needed to define what is meant by "System Hardening."

Except for the comments regarding the definitions for VCA, SCI, EAP, PCA, and ERC as noted above in Question 1-6, SPP supports the changes the SDT has made to the Requirements for CIP-007.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

If a firewall has VLANs on it for medium and low, or high and low, does that pull low impact network connection into scope because it shares the same firewall? More clarity is nedded.

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

Part 5.1 – The replacement of 'where technically feasible' with 'per system capability' could potentially introduce risk. TFEs require additional mitigations to address the risk posed by not requiring authentication - per system capability does not have this requirement.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.

Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
While NST endorses replacing "where technically feasible" with "per system capability" in R.1.1, we believe the proposed new language in R1.1 ("Disable or prevent unneeded routable protocol network accessibility") subtracts rather than adds clarity, and we therefore recommend retaining the existing and familiar "enable only logical network accessible ports." If the SDT wants to explicitly allow for the use of host-based firewalls or similar, per device controls as an alternative, R1.1 could be modified to say, "enable only logical network accessible ports... or prevent access to unnecessary logical network accessible ports using host-based firewalls or other, per device controls."	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices. Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	No
Document Name	

Comment

While AEP agrees with most of the proposed revisions in CIP-007-7, we recommend adding languages to Requirement R1 Part 1.3 to provide more clarity. Requirement R1 Part 1.3 would then read “*Mitigate the risk of CPU or memory vulnerabilities by* ***(1)*** *preventing the sharing of CPU and memory resources between VCAs or* ***(2) protecting all VCA on SCI with the highest impact BCS rating*** *that are not of, or associated with, the same impact categorization.*”

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- NEE supports the NPCC Comments:
- Request clarification of CIP-007, Part 1.3. It appears that applications operating on a SCI platform where memory and CPU hardware devices are shared MUST all be classified at the same impact level. Is this a correct interpretation? If not, please explain. Memory and CPU are both implemented in hardware devices which are naturally shared across multiple processes and system functions. There is no known method to prevent the physical sharing of memory and CPU hardware devices in a virtual platform (SCI) based on the application and operating system processes that share these hardware devices.
- Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	No
Document Name	

Comment

CHPD agrees with the proposed changes to Requirement R1.1 however, CHPD does not agree with the proposed changes to Requirement R1.3.

Regarding Requirement R1.3, CHPD firmly believes there has been no demonstrated risk of hardware-based virtualization attacks that warrant this requirement. CISA's Known Exploited Vulnerabilities Catalog | CISA only lists a single VM escape vulnerability, which was patched before it was disclosed, and is disputed by the vendor as being in the wild. While a number of VM escape techniques have been disclosed, all have been patched and saw no confirmed exploitation in the wild.

Even speculative execution vulnerabilities like Spectre and Meltdown have not seen any confirmed exploitation in the wild and are effectively patched. Future vulnerabilities can be effectively managed by a Responsible Entity's CIP-007 R2 patching program (or mitigated by a mitigation plan if patching is not possible) and CIP-010 R3 Vulnerability Assessment program. This requirement only serves to restrict entities on architectures and to increase the cost of virtualization which would make it untenable.

We can also look to NIST 800-125A, Security Recommendations for Server-based Hypervisor Platforms. While VM Process Isolation is considered the first and possibly most important of the baseline functions, preventing VMs from sharing CPU or memory is not listed as any of the security recommendations to secure hypervisor baseline functions.

Looking to the technical aspects, this requirement misuses the functionality of DRS (or similar for non-VMware vendors) in ways that were not intended. DRS affinity rules were not intended as a cyber security tool to prevent side channel attacks, but are intended to ensure availability and performance of VMs, as DRS is fundamentally a tool to allocate distributed resources. There are typically three types of rules; VM-to-VM affinity rules which ensure VM stay together for performance reasons, VM-to-VM anti-affinity rules which ensure that VMs stay apart for redundancy reasons incase a host fails, and VM-to-host rules, which ensure that VMs either stay connected to a specific physical resource. Because DRS rulesets were not intended for security, affinity rules do not generally allow you to specify groups of VMs and cannot share CPU with another group of VMs. That means, for example, an EACMS VM would need to have a rule for every VM that it cannot share CPU and memory with to comply with this requirement. If a Responsible Entity were to do this, this would create a massive web of affinity rules that would be unmanageable and potentially create a reliability issue in the event of a hardware failure, where critical VMs might not be able to find a suitable host to run on given affinity restrictions.

Setting aside the security and technical problems, the requirement itself is not clear in what it allows. It is possible to interpret the requirement as contradicting the definition of SCI. There is a very fine line drawn with the terminology in the definition of SCI ("cluster") and the wording of CIP-007 R1.3 (sharing of CPU and memory). Some might interpret the specific hosts allowed to host CIP devices (according to the affinity ruleset) as the "cluster", meaning that R1.3 essentially contradicts the definition of SCI. There is also the question of if a high watermarked BCA still counts as its Medium Impact self. Even though you must treat it as a high impact PCA, it is still fundamentally a medium impact BCA and according to the requirement, it cannot coexist on the same CPU and memory as it is of a different impact classification. The language of R1.3 combined with the definition of SCI creates too vague of a security control to implement without significant compliance risk.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Definitions such as VCA is not clear and confusing.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Please provide the technical guidelines within the standard document. SRP feels they are necessary to understand this requirement in more detail. Regarding R1.3 please clarify the expectation around not sharing CPU and Memory and it still be SCI and definition for SCI. What role does storage play?	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
For Requirement R1.3, consider if there is a better verb than “preventing” when discussing mitigation of risk (in order to avoid potential overly prescriptive interpretations and enforcement). Further, we are concerned about the last phrase in Requirement R1.3, “between VCAs that are not of, or associated with, the same impact categorization.” We question whether this phrase is needed in the requirement language and, if included, whether it could force Entities to “cluster” virtual assets by impact level (high, medium, low) which would be inefficient. We are supportive of operating to the “high water” level; we are simply concerned about the categorization level. We recommend re-wording the proposed requirement text to read, “Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources between unassociated VCAs that are not of, or associated with, the same SCI (clustered configuration).” [changes underlined]	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

See EEI comment.

Likes 0	
Dislikes 0	

Response

Alison Mackellar - Constellation - 5

Answer	Yes
Document Name	

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	Yes
Document Name	

Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Request clarification of CIP-007, Part 1.3 since there are two scenarios. In the first scenario there is one SCI for everything - BES Cyber Assets, PCAs, EACMS, PACS, potentially non-CIP VMs. In the second scenario there are two SCIs. The first SCI includes BES Cyber Assets and PCAs (within the ESP). The second SCI includes assets outside the ESP, like EACMS, PACS, potentially non-CIP VMs. These two SCIs do not have the same risk. Should we expect different Requirements for these two SCIs?	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the proposed changes to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	

Comment

Comments: For Requirement R1.3, consider if there is a better verb than “preventing” when discussing mitigation of risk (in order to avoid potential overly prescriptive interpretations and enforcement).

Further, we are concerned about the last phrase in Requirement R1.3, “between VCAs that are not of, or associated with, the same impact categorization.” We question whether this phrase is needed in the requirement language and, if included, whether it could force Entities to “cluster” virtual assets by impact level (high, medium, low) which would be inefficient. We are supportive of operating to the “high water” level; we are simply concerned about the categorization level.

It is our understanding that if everything in an asset is operated or associated at the same impact level, then the asset does not meet the proposed definition of SCI. It is also our understanding that the proposed Requirement 1 Part 1.3 is intended to be backwards-compatible and to not require that present-day compliant network architecture change. However, we were not clear on these points just from reading the proposed revised text alone. We urge the SDT to issue additional clarity on these points, either through documented technical guidance or even clarifying changes to the proposed requirement text itself.

Likes 0	
Dislikes 0	

Response

patricia ireland - DTE Energy - 4

Answer	Yes
Document Name	

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CEHE agrees with the proposed revisions in CIP-007.

Likes 0	
Dislikes 0	

Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	
While we agree with the changes as a whole, consider clarifying what memory means in CIP-007 R1.3. Does memory refer to RAM?	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the revised proposed changes to the CIP-007 standard.	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
LES agrees with the majority of proposed changes regarding CIP-007 but has concerns with the ‘Technical Feasibility’ conforming change which is further detailed in the Question 11 response.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE recommends removing the language “Mitigate the risk of CPU or memory vulnerabilities” in CIP-007 Part 1.3 as it is more appropriate for Technical Rationale.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Joni Jones - Wabash Valley Power Association - 1	
Answer	Yes

Document Name	
Comment	
no further comments	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

9. The SDT revised CIP-010 R1 to focus on defining change, authorizing change, and verifying that CIP-005 and CIP-007 related security controls are not affected by changes. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

The verbiage pertaining to CIP-005 and CIP-007 controls within CIP-010 R1 is acceptable. However, the verbiage in CIP-010 R1.2.1 states, "Prior to implementing *ANY* change…" which is far too all-inclusive. Additionally, the verbiage in CIP-010 R2.1 states, "Methods to monitor for unauthorized changes…" which also implies that ANY change is included in this scenario. The verbiage in both R1.2.1 and R2.1 should be revised to include only those changes applicable to Part 1.1 of CIP-010, not ANY change, as it is currently stated/implied.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

The verbiage pertaining to CIP-005 and CIP-007 controls within CIP-010 R1 is acceptable. However, the verbiage in CIP-010 R1.2.1 states, "Prior to implementing *ANY* change…" which is far too all-inclusive. Additionally, the verbiage in CIP-010 R2.1 states, "Methods to monitor for unauthorized changes…" which also implies that ANY change is included in this scenario. The verbiage in both R1.2.1 and R2.1 should be revised to include only those changes applicable to Part 1.1 of CIP-010, not ANY change, as it is currently stated/implied.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Please provide the technical guidelines within the standard document. On “The Measures”, they call out testing what used to be in “The Requirements”, does this mean for each type of change there needs to be a different set of cyber security controls tested.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	No
Document Name	

Comment

By removing the baseline requirement would leave too much ambiguity in the standard versus the more prescriptive requirements that are there now. Ambigous requirements relys on too much auditor interpretation. Can the SDT develop a pactice or implementation guidance. Industry needs to understand whats acceptable and whats not.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1, Group Name Eversource Group

Answer	No
Document Name	

Comment

There is concern that the revised CIP-010-5 is not backwards compatible. For instance even though the Technical Rationale for CIP-010-5 states on page 5:

'The items found in the CIP-010-4 **“baseline” are now included in the Measures column within CIP-010-5**. This maintains compatibility with current state but allows flexibility for virtualization technologies. This also ensures the focus is not on documenting past changes but the authorization of current or future changes, thus making the requirement forward looking with a clearer security objective'

The actual CIP-010-5 **only mentions baseline once in the Measures column, for R1.3**

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Definitions such as SCI is not clear and confusing.	
Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE is concerned security obligations will be reduced by removing an explicit requirement for Registered Entities to create and maintain baseline configuration documentation. Establishing and maintaining baseline configurations represent best practices for system hardening. Texas RE recommends adhering to NIST Special Publication 800-53 (Rev. 5), CM-2 Baseline Configuration, which states, “Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.” NIST Special Publication 800-53 (Rev. 5) provides additional information, such as using tools to track version numbers on operating systems, applications, types of software installed, and current patch levels in order to maintain the currency, completeness, accuracy, and availability of the baseline configurations of systems. This is information that is currently captured within existing baseline documentation requirements. If the drafting team has concerns that maintaining baseline documentation of dynamic VMs is not technically feasible, Texas RE suggests adding the verbiage “per system capability” to CIP-010 R1’s baseline requirements. Registered Entities have demonstrated that the vast majority of systems, both physical and virtual, are capable of having baseline documentation created, tracked, and updated as necessary. As such, this requirement should remain in place for those systems where it is technically feasible to perform this industry best security practice.	
Likes 0	
Dislikes 0	
Response	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	No
Document Name	

Comment

CHPD approves of the approach, but finds several fundamental issues with this draft.

By including the previous baseline items in the Measure, the intented goal is not met. No Responsible Entity's compliance staff will be willing to risk doing any less than what is listed in the Measures. If the SDT wants to commit to allowing Responsible Entities to choose their own changes that CIP-010 R1 applies to, it should consider removing the configuration items from the Measures. It will then need to be up to NERC and the Regional Entities to ensure that Responsible Entities are appropriately determining the changes that apply.

Given that software is effectively being removed from R1.1, it does not make sense to perform verification of software integrity and source (R1.5) in CIP-010 R1. It should instead be moved to a different requirement (either a new requirement in CIP-010 or into CIP-013).

CHPD believes that the changes proposed to CIP-010 R1 creates problems to CIP-010 R2.1. A change is fundamentally a difference from what something was previously to what something is now. You fundamentally have to know what something was to tell if it has changed. Knowing the previous state of the system is fundamentally what a baseline configuration is, and that makes it impossible to detect a change without having a baseline configuration. A Responsible Entity might be able to configure events to detect when certain changes occur, but that alert needs to know what the previous state was to know if a change occurred.

If the SDT wishes to pursue the current language, it will need to either eliminate CIP-010 R2 or rewrite it, as it is not possible to comply with it without tracking a baseline configuration. In keeping with the actual security objective of CIP-010 R1 (ensuring changes do not impact security controls adversely) CHPD recommends looking to TOP-001-4 R21/R24 for guidance. Instead of detecting unauthorized changes, require that RE's perform a test of a subset of CIP-005 and CIP-007 cyber security controls on a periodic basis.

Alternatively, the SDT could keep the baseline configuration requirements, reordering the requirements and removing time frames, and eliminating the proscriptive list of configuration items and allowing Responsible Entities to determine the configuration items for themselves.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

Comments:

- CIP-010-5 R1 P1.1 Please add “per system capability”. Proposed language: “Define types of changes that may impact CIP-005 or CIP-007 security controls per system capability. For those changes:” The reasoning is that most network CA or VCA could only “baseline” firmware and logically accessible network ports. The security patches will be part of the firmware.

- CIP-010-5 R1 P1.1.1 and P1.1.3 Please add “per system capability”.
- 1.1.1. Prior to change implementation, identify impacted security controls in CIP-005 and CIP-007 per system capability, except during CIP Exceptional Circumstances.
- 1.1.3. Verify cyber security controls from CIP-005 and CIP-007 per system capability are not adversely affected.
- CIP-010-5 R1 P1.1.3 Measure please include in bullet 2 “or baseline tool” to read as follows: “An output from cyber security testing tools such as a vulnerability scanner or baseline tool.”
- Removing baseline language and concept from the standard completely creates risks for Entities to demonstrate compliance through the transition. The addition of all CIP-005 and CIP-007 controls as potential baselines or monitoring may take entities more than 12-months and therefore supports a 36-month implementation plan to migrate a large number of cyber assets.
- CIP-010-7 R1 P1.1 is a migration toward objected focus for CIP-005 and CIP-007 security controls but clarity on the Entities’ definition or determination of impact based up technology will take time and tooling requiring more time than 12-month implementation period. Objectives should be clear and must be applied based per the system capability.

Likes 0	
Dislikes 0	

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

The revised CIP-010 R1.1 language is vague and allows each entity to choose different types of changes to manage. What if a change occurs that affects the security controls; however, this change was not previously defined as a type of change that may impact CIP-005 or CIP-007? The removal of the specific baseline requirements will lead to a broad interpretive field on what is actually required and what is not. This may lead to differing regional interpretations and each entity left unclear as to what they have to do and what is merely good practice or due diligence.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

The revised CIP-010 R1.1 language is vague and allows each entity to choose different types of changes to manage. What if a change occurs that affects the security controls; however, this change was not previously defined as a type of change that may impact CIP-005 or CIP-007? The removal of the specific baseline requirements will lead to a broad interpretive field on what is actually required and what is not. This may lead to differing regional interpretations and each entity left unclear as to what they have to do and what is merely good practice or due diligence.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP appreciates SDT’s attempt in making CIP-010-5 Requirement 1 Part 1.1 less prescriptive by moving types of baseline changes from the Requirements column to the Measures column. However, AEP believes this proposed revision may have unintended consequences of broadening the scope by not providing a definitive list to the Registered Entities. Therefore, AEP recommends moving the bulleted items from the Measures column to the Requirements column. AEP also recommends not including “*Any other configuration or setting determined by the Responsible Entity*” as this introduces ambiguity.

The Requirement 1 Part 1.1 would read as follows:

“***Types*** *of changes that may impact CIP-005 or CIP-007 security controls* ***shall include the following items:***

- ***Operating system (OS) software;***
- ***Firmware, where no independent OS exists;***
- ***Commercially available or opensource application software, including application containers;***
- ***Custom software installed, including application containers;***
- ***Configuration that modifies network accessible logical ports or network accessible services on an Applicable System;***
- ***SCI configuration of host affinity control between systems with different impact ratings;***
- ***Changes to configurations or settings for an ESP between systems with different impact ratings; or***
- ***Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations.***

For those changes:

1.1.1. Prior to change implementation, identify impacted security controls in CIP-005 and CIP-007, except during CIP Exceptional Circumstances;

1.1.2. Authorize those changes; and

1.1.3. Verify cyber security controls from CIP-005 and CIP-007 are not adversely affected.”

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

Recommend keeping the approved language (keeping baselining) instead of the proposed update because 1) the older language better improves reliability (security) and 2) the newer language introduces more uncertainty in tracking the baseline. We suggest the existing group approach addresses this overall concern. We understand the new language tries addressing the brief period where an entity moves from one baseline to another. Meaning the entity has two baselines during this transition. We suggest there are other, less impactful ways to address these transitions.

Also, removing baselining causes so many questions and complications. Suggest the proposed updates do not simplify, instead these updates 1) add complexity, 2) increase cost with questionable benefit and 3) increase uncertainty of audit interpretations. Suggest that the SDT address previous baseline concerns in other ways. The concern for baselining system operator virtual desktops could be addressed by baselining the underlying disk image. The concern of children VMs not updating when their parents are updated could be addressed by documenting those situations.

Recommend keeping the approved language because the changes are not backward compatible.

Request Supply Chain updates align with Supply Chain best practices (like NIST 800-161)

The following comments provide reasons to support returning the approved baselining language.

Recommend an update to CIP-010 R1. This proposed removes the approved language on custom software. Request written exclusion of custom software in R1. Making this change reduces the ripple effect on the sub-parts of R1. As written, the proposed language impacts change process and change documentation. The proposed R1.3 adds confusion on software vs firmware. In the proposed updates, R1.3 is the only Requirement for tracking *all* versions.

For CIP-010, Part 1,1, we 1) recommend an update to provide audit certainty as to who determines impactful changes. Recommend adding “as determined by entity” to the Requirement language - “Define types of changes that may impact CIP-005 or CIP-007 security controls. For those changes:” and 2) request clarification. If the SDT moves towards measurable objective based, where are the objectives? As written, CIP-010 could be a heavy lift when getting into the details.

Request clarification of CIP Exceptional Circumstances in CIP-010, Part 1.1.1. Is this exception intended to be specific (Part 1.1.1) or general (R1)?

In CIP-010 Part 1.3, we 1) recommend moving “(or firmware where no OS exists)” from Requirements to Measures because the proposed language is confusing; 2) request explicit clarification that firmware is software; and 3) request update to Measures. Since “baseline” was removed from the Requirements, the Measures should not include “baseline.”

Likes 0	
Dislikes 0	

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer	No
Document Name	

Comment

R1 Part 1.3: With the removal of the specific baseline references for which changes are relevant to R1 Part 1.3 (previously R1.6), Tacoma Power is concerned that custom software (scripts) could be identified as applicable.

Likes 0

Dislikes 0

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST believes proposed changes beyond those needed for conformance have little or nothing to do with virtualization, are unlikely to improve anyone’s cyber security posture, are outside the scope of the original 2016 SAR, are not addressed in any relevant FERC Order, and would be an unnecessary and unwelcome distraction for entities trying to adjust their CIP programs and documentation to accommodate new virtualization-related requirements. NST remains unconvinced that the existing requirement to maintain configuration baselines would inhibit the use of virtualized environments or that it has somehow become an outmoded approach to change management. We note that the NIST Cyber Security Framework, which has some strong advocates among various bodies with electric utility industry and reliability standard oversight responsibilities, lists among its controls, "A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)." We note, further, an online glossary accessible on the vmware.com web site includes an entry that reads, "A Configuration management system allows the enterprise to define settings in a consistent manner, then to build and maintain them according to the established baselines.”

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Recommend keeping the approved language (keeping baselining) instead of the proposed update because 1) the older language better improves reliability (security) and 2) the newer language introduces more uncertainty in tracking the baseline. We suggest the existing group approach addresses this overall concern. We understand the new language tries addressing the brief period where an entity moves from one baseline to another. Meaning the entity has two baselines during this transition. We suggest there are other, less impactful ways to address these transitions.

Also, removing baselining causes so many questions and complications. Suggest the proposed updates do not simplify, instead these updates 1) add complexity, 2) increase cost with questionable benefit and 3) increase uncertainty of audit interpretations. Suggest that the SDT address previous baseline concerns in other ways. The concern for baselining system operator virtual desktops could be addressed by baselining the underlying disk image. The concern of children VMs not updating when their parents are updated could be addressed by documenting those situations.

Recommend keeping the approved language because the changes are not backward compatible.

Request Supply Chain updates align with Supply Chain best practices (like NIST 800-161)

The following comments provide reasons to support returning the approved baselining language.

Recommend an update to CIP-010 R1. This proposed removes the approved language on custom software. Request written exclusion of custom software in R1. Making this change reduces the ripple effect on the sub-parts of R1. As written, the proposed language impacts change process and change documentation. The proposed R1.3 adds confusion on software vs firmware. In the proposed updates, R1.3 is the only Requirement for tracking *all* versions.

For CIP-010, Part 1,1, we 1) recommend an update to provide audit certainty as to who determines impactful changes. Recommend adding “as determined by entity” to the Requirement language - “Define types of changes that may impact CIP-005 or CIP-007 security controls. For those changes:” and 2) request clarification. If the SDT moves towards measurable objective based, where are the objectives? As written, CIP-010 could be a heavy lift when getting into the details.

Request clarification of CIP Exceptional Circumstances in CIP-010, Part 1.1.1. Is this exception intended to be specific (Part 1.1.1) or general (R1)?

In CIP-010 Part 1.3, we 1) recommend moving “(or firmware where no OS exists)” from Requirements to Measures because the proposed language is confusing; 2) request explicit clarification that firmware is software; and 3) request update to Measures. Since “baseline” was removed from the Requirements, the Measures should not include “baseline.”

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

Do not agree with the proposed CIP-010 R1.2 which states “Prior to implementing any change in the production environment” security controls testing is required. The use of “any change” is overly inclusive and would require security controls testing and compliance documentation for changes that would not fall into scope of the required change review/testing/authorizations identified in the proposed CIP-010 R1.1. Propose including language for this requirement to tie back to the types of changes identified in CIP-010 R1.1.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

R1-Removing baseline configuration does not change what needs to be done in practice. Entities will still need to retain a baseline configuration as evidence from which to establish the changes that were authorized.

- For Part 1.1 an entity will still need to show the baseline configuration prior to the change to show required cyber security controls in CIP-005 and CIP-007 are not adversely affected.

- For Part 2.1 an entity will still need to provide baseline configurations for evidence that they monitor at least once every 35 calendar days for unauthorized changes to the items listed Parts 1.1 and 1.2.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

R2.1 ties back to R1. Please specify which components we need at a minimum to monitor for the unauthorized changes? Otherwise, it is up to the auditor’s discretion.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer	No
Document Name	

Comment

SPP does not agree with the proposed changes to CIP-010 R1. Specifically, SPP believes that the current language improves reliability (security) but that the proposed language introduces more uncertainty in tracking the baseline. As such, the SPP recommends retaining the currently approved language for CIP-010 and not moving the prior langue to the measures.

Additionally, the changed proposed for R1.3 are confusing. The way the SDT has written R1.3 language, the requirement appears to only apply to changes to software or firmware versioning, rather than new software. Finally, the proposed measures for R1.3 do not match with the proposed R1.3 requirement language.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
IESO supports the comments provided by NPCC and IRC	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	
We have concerns with the SCI definition and it potentially bringing additional devices into scope. Additionally WEC agrees with NSRF comments regarding R1: *The SDT needs to revisit the issue of discussing a baseline in the R1 language. While we appreciate the difficulty in maintaining a traditional baseline when employing virtualization, and while we approve more flexible requirement language, it appears from industry comments and questions that simply removing the phrase “baseline” has caused confusion. This implies that there will be confusion in the future in terms of auditing and enforcement. Perhaps the term “baseline” should be re-added to the Measure as it pertains to traditional, non-virtual systems and then provide additional Measures for virtual systems.*	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	

Answer	No
Document Name	
Comment	

Recommend keeping the approved language (keeping baselining) instead of the proposed update because 1) the older language better improves reliability (security) and 2) the newer language introduces more uncertainty in tracking the baseline. We suggest the existing group approach addresses this overall concern. We understand the new language tries addressing the brief period where an entity moves from one baseline to another. Meaning the entity has two baselines during this transition. We suggest there are other, less impactful ways to address these transitions.

Also, removing baselining causes so many questions and complications. Suggest the proposed updates do not simplify, instead these updates 1) add complexity, 2) increase cost with questionable benefit, and 3) increase uncertainty of audit interpretations. Suggest that the SDT address previous baseline concerns in other ways. The concern for baselining system operator virtual desktops could be addressed by baselining the underlying disk image. The concern of children's VMs not updating when their parents are updated could be addressed by documenting those situations.

Recommend keeping the approved language because the changes are not backward compatible.

Request Supply Chain updates align with Supply Chain best practices (like NIST 800-161)

The following comments provide reasons to support returning the approved baselining language.

Recommend an update to CIP-010 R1. This proposed removes the approved language on custom software. Request written exclusion of custom software in R1. Making this change reduces the ripple effect on the sub-parts of R1. As written, the proposed language impacts the change process and change documentation. The proposed R1.3 adds confusion on software vs firmware. In the proposed updates, R1.3 is the only Requirement for tracking *all* versions.

For CIP-010, Part 1,1, we 1) recommend an update to provide audit certainty as to who determines impactful changes. Recommend adding “as determined by entity” to the Requirement language - “Define types of changes that may impact CIP-005 or CIP-007 security controls. For those changes:” and 2) request clarification. If the SDT moves towards measurable objective-based, where are the objectives? As written, CIP-010 could be a heavy lift when getting into the details.

Request clarification of CIP Exceptional Circumstances in CIP-010, Part 1.1.1. Is this exception intended to be specific (Part 1.1.1) or general (R1)?

In CIP-010 Part 1.3, we 1) recommend moving “(or firmware where no OS exists)” from Requirements to Measures because the proposed language is confusing; 2) request explicit clarification that firmware is software, and 3) request an update to Measures. Since “baseline” was removed from the Requirements, the Measures should not include “baseline.”

Likes 0	
Dislikes 0	
Response	

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	
Comment	

We support NPCC TFIST comments.

Recommend keeping the approved language (keeping baselining) instead of the proposed update because 1) the older language better improves reliability (security) and 2) the newer language introduces more uncertainty in tracking the baseline. We suggest the existing group approach addresses this overall concern. We understand the new language tries addressing the brief period where an entity moves from one baseline to another. Meaning the entity has two baselines during this transition. We suggest there are other, less impactful ways to address these transitions.

Also, removing baselining causes so many questions and complications. Suggest the proposed updates do not simplify, instead these updates 1) add complexity, 2) increase cost with questionable benefit and 3) increase uncertainty of audit interpretations. Suggest that the SDT address previous baseline concerns in other ways. The concern for baselining system operator virtual desktops could be addressed by baselining the underlying disk image. The concern of children VMs not updating when their parents are updated could be addressed by documenting those situations.

Recommend keeping the approved language because the changes are not backward compatible.

Request Supply Chain updates align with Supply Chain best practices (like NIST 800-161)

The following comments provide reasons to support returning the approved baselining language.

Recommend an update to CIP-010 R1. This proposed removes the approved language on custom software. Request written exclusion of custom software in R1. Making this change reduces the ripple effect on the sub-parts of R1. As written, the proposed language impacts change process and change documentation. The proposed R1.3 adds confusion on software vs firmware. In the proposed updates, R1.3 is the only Requirement for tracking *all* versions.

For CIP-010, Part 1,1, we 1) recommend an update to provide audit certainty as to who determines impactful changes. Recommend adding “as determined by entity” to the Requirement language - “Define types of changes that may impact CIP-005 or CIP-007 security controls. For those changes:” and 2) request clarification. If the SDT moves towards measurable objective based, where are the objectives? As written, CIP-010 could be a heavy lift when getting into the details.

Request clarification of CIP Exceptional Circumstances in CIP-010, Part 1.1.1. Is this exception intended to be specific (Part 1.1.1) or general (R1)?

In CIP-010 Part 1.3, we 1) recommend moving “(or firmware where no OS exists)” from Requirements to Measures because the proposed language is confusing; 2) request explicit clarification that firmware is software; and 3) request update to Measures. Since “baseline” was removed from the Requirements, the Measures should not include “baseline.”

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

We are uncomfortable with the slight ambiguity of the language. To make us more comfortable with the language, please define more clearly CIP-005 and CIP-007 security controls (Example: CIP-007 R1: Logical vs physical ports).

Likes 0	

Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	No
Document Name	
Comment	
R1 Part 1.3: With the removal of the specific baseline references for which changes are relevant to R1 Part 1.3 (previously R1.6), Tacoma Power is concerned that custom software (scripts) could be identified as applicable.	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	No
Document Name	
Comment	
From a security perspective, it is not clear what the proposed wording in CIP-010 R1.1 is intended to accomplish. The proposed wording doesn’t look like it belongs in a change control requirement. Having a baseline and monitoring a baseline is one of the strongest security controls that exist in the CIP Standards. The proposed language in the requirements does not provide much direction and without reading the measures, an entity would have no idea how to interpret the requirement or how it relates to security of configuration management. SMUD recommends reconsidering the objective being addressed for changing CIP-010 R1.1 as the new direction proposed seems to lack clarity on the intent. It is not clear how the changes being made are needed to support virtualization. SMUD’s recommendation is to leave the requirements as they are unless there is a specific need to address a requirement in support of virtualization technology - this does not appear to be the case.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	

Comment

We support NPCC RSC's comments.

Propose changing software (or firmware where no OS exists) to software or firmware. Hardware that runs an OS also has firmware that can usually be updated

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer	No
Document Name	

Comment

The SRC does not agree with the proposed changes to CIP-010 R1. Specifically, the SRC believes that the current language better improves reliability (security) and the proposed language introduces more uncertainty in tracking the baseline. As such, the SRC recommends retaining the currently approved language.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring

Answer	Yes
Document Name	

Comment

WECC supports the proposed changes but has some minor suggestions for possible edits.

Minor suggest edit, but to be consistent with the language of R1, Part 1.1 consider changing the language in the Measure from:

‘a documented process that defines changes that may impact security controls in CIP-005 and CIP-007, such as but not limited to:’

To:

a documented process that defines changes that may impact CIP-005 and CIP-007 security controls, such as but not limited to:

Likes 0	
Dislikes 0	

Response	
Joni Jones - Wabash Valley Power Association - 1	
Answer	Yes
Document Name	
Comment	
Recommend removing R1.1.1. As written, R1.1 says What do you think will happen, authorize, test what did happen (regardless of what you thought would happen). While advance thought is good practice, the document what you think will happen is nothing more than a checkbox requirement that does not improve security.	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF). For the proposed CIP-010-5, R1, Part 1.1.1, the draft language clarifies that impacted security controls in CIP-005 and CIP-007 must be identified prior to the change. Does the inclusion of the “prior to change” language in part 1.1.1 imply that the authorization of changes in part 1.1.2 can occur before *or* after the change? If the intent is to require authorization prior to the change, then the requirements should clearly state this.	
Likes 0	

Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes removing the 30 day timeframe and baseline requirements gives the Change & Configuration Management Program greater flexibility.	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
While LES is in agreement with the flexibility offered through the proposed changes, the abrupt shift away from baselines could use additional clarity for entities continuing to utilize the existing baseline method such as including baselines as an existing measure.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that changes to CIP-010 R1 help streamline changes that are routine and known to not impact security controls. Allows effort to be focused on risk-based changes.	
Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer	Yes
Document Name	

Comment

We agree and are very favorable of the revisions made to CIP-010 R1. As a quick note, part 1.6 should say part 1.3 in R1.3.

Likes 0	
Dislikes 0	

Response

patricia ireland - DTE Energy - 4

Answer	Yes
Document Name	

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	Yes
Document Name	

Comment

BC Hydro agrees with the proposed changes. However, BC Hydro has some concerns on the understanding specific to CIP-010 R1.3 which should clearly indicate that only the identified impacted security controls from CIP-010 Part 1.1.1 should be verified. Additionally, it is not clear if the verification can be done on a test asset/system or if it is expected to be done on all production assets of a given system.

The new CIP-010 R1.2.1 implies that the verification for CIP-010 R1.1.3 can be done on a representative test asset/system instead of all production assets for the given system. Testing on all production assets could have huge resourcing impacts.

BC Hydro seeks clarification on the above points and suggest adding an explanation in the technical rationale of the revised CIP-010 standard.

Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Comments: The SDT needs to revisit the issue of discussing a baseline in the R1 language. While we appreciate the difficulty in maintaining a traditional baseline when employing virtualization, and while we approve more flexible requirement language, it appears from industry comments and questions that simply removing the phrase “baseline” has caused confusion. This implies that there will be confusion in the future in terms of auditing and enforcement. Perhaps the term “baseline” should be re-added to the Measure as it pertains to traditional, non-virtual systems and then provide additional Measures for virtual systems.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the revision of CIP-010 R1 to focus on CIP-005 and CIP-007 related security controls are not affected by changes.	

Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	

Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	

See EEI comment.

Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

Alliant Energy supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
The SDT needs to revisit the issue of discussing a baseline in the R1 language. While we appreciate the difficulty in maintaining a traditional baseline when employing virtualization, and while we approve more flexible requirement language, it's evidence from industry comments and questions that simply removing the phrase "baseline" out completely has caused confusion. This implies that there will be confusion in the future in terms of auditing and enforcement. Perhaps the term "baseline" should be re-added to the Measure as it pertains to traditional, non-virtual systems and then provide additional Measures for virtual systems.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	

Comment

Exelon will align with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

10. The SDT made other revisions to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer	No
Document Name	

Comment

The SRC does not agree with the other key proposed changes to CIP-010. Specifically, the SRC believes that within R2, the term “Unauthorized changes” is too broad and does not include “per system capability.” The SRC recommends for the SDT to consider adding “monitor for changes identified in R1.1.” The SRC also requests further clarification regarding the proposed change to R3.3 in regards to when a system becomes an “Applicable System.” The SRC recommends that STD clarify whether this occurs before / after engaging service provision. The SRC agrees with the proposed changes to the remaining sub-requirements.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

We support NPCC RSC's comments.

In R2.1 The use of the term “for unauthorized changes” without the reference to a defiined set of changes like the previous baseline, could imply that the entity authorize all changes on the system. This could include addition of data to existing or new files. Changing of file dates. Configuration of windows layouts on a display…..

In R3.3, make “Cyber System” singular for both uses in the first bullet or better yet, use Applicable Sytem since the defintion of Cyber Sytem includes PACS and the Applicable Systems do not

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5,

6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley

Answer	No
Document Name	

Comment

Given the ambiguity of CIP-010 R1.1 it is difficult to understand why the other sub-requirements were either removed or updated. It also makes no sense to modify R1.1 in the way that it was modified, yet keep R2.1 relatively unchanged. Does R2.1 now mean that the entire system and all apps need to be monitored for unauthorized changes? It is unclear what unauthorized changes are to be monitored in the new version. The current version of the standard makes it clear what needs to be monitored.

SMUD does not agree with putting the requirements in the measures which seems to be what is happening here. We recommend rolling CIP-010 R1.1 back to what it was as these changes do not support virtualization.

Likes 0	
Dislikes 0	

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer	No
Document Name	

Comment

Tacoma Power is concerned that the scope of change associated to CIP-010-5 R2 part 2.1 is no longer bounded. The current version of CIP-010 R2 Part 2.1 is scoped to only those “changes to baseline configuration (as described in Requirement R1, Part 1.1).”

Tacoma Power suggests the following modification to the proposed language of CIP-010-5 R2 Part 2.1:
“Methods to monitor for unauthorized changes that may impact CIP-005 or CIP-007 security controls (as described in Requirement R1, Part 1.1) at least once every 35 calendar days. Document and investigate detected unauthorized changes.”

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

R1.1: We are uncomfortable with the slight ambiguity of the language. To make us more comfortable with the language, please define more clearly CIP-005 and CIP-007 security controls (Example: CIP-007 R1: Logical vs physical ports). R1.2: Like the clear documentation and the ability to use CIP exceptional circumstances. R2.1: Why did they add the word methods (under requirements)?. We are comfortable with the rest of the requirements.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support NPCC TFIST comments.

In CIP-010, Part 2.1, request clarification of the SDT’s intent. Does the new language pertain to 1) version changes in 1.3, 2) changes for CIP-005 & CIP-007 or 3) both?

In CIP-010, Part 3.3, Request clarification on when “Applicable System” starts. Suggest changing the beginning of Requirement from “Prior to becoming a new Applicable System” to “Prior to becoming a new, production Applicable System”

In CIP-010, Attachment 1, 1.3 we recommend removing two bullets because they are not software vulnerability mitigation which is the title of 1.3. The new bullet which is “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution.” The second bullet is “System hardening.” Also, the new bullet preserves the vulnerability which is contrary to good security. The last bullet should remain since it covers alternatives.

In CIP-010, Attachment 1, 1.4 we recommend removing two bullets because they are not mitigating the introduction of malicious code which is the title of 1.4. The new bullet which is “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code.” This new bullet preserves the vulnerability which is contrary to good security. The second bullet is “Application whitelisting;” The last bullet should remain since it covers alternatives.

Since CIP-010, Attachment 2 is the Measures for CIP-010, Attachment 1, we request updates to Attachment 2 per our Attachment 1 comments

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

In CIP-010, Part 2.1, request clarification of the SDT’s intent. Does the new language pertain to 1) version changes in 1.3, 2) changes for CIP-005 & CIP-007 or 3) both?

In CIP-010, Part 3.3, Request clarification on when “Applicable System” starts. Suggest changing the beginning of Requirement from “Prior to becoming a new Applicable System” to “Prior to becoming a new, production Applicable System”

In CIP-010, Attachment 1, 1.3 we recommend removing two bullets because they are not software vulnerability mitigation which is the title of 1.3. The new bullet is “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution.” The second bullet is “System hardening.” Also, the new bullet preserves the vulnerability which is contrary to good security. The last bullet should remain since it covers alternatives.

In CIP-010, Attachment 1, 1.4 we recommend removing two bullets because they are not mitigating the introduction of malicious code which is the title of 1.4. The new bullet is “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code.” This new bullet preserves the vulnerability which is contrary to good security. The second bullet is “Application whitelisting;” The last bullet should remain since it covers alternatives.

Since CIP-010, Attachment 2 is the Measures for CIP-010, Attachment 1, we request updates to Attachment 2 per our Attachment 1 comments.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	No
Document Name	

Comment

Please refer to the response to question #9.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

IESO supports the comments provided by NPCC and IRC

Likes 0	

Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	No
Document Name	

Comment

AWS agrees with changes to CIP-010 R1, R2, and R3. AWS is concerned that CIP-010 R4 does not address security risk associated with virtual machines hosted on physical Transient Cyber Assets because the standard language states that a VM running on a physical TCA can be treated as software. The Standard allows an entity to choose one or a combination of security controls that may not extend cyber security protections to the VM itself leaving VMs potentially vulnerable to security threats undetected by the physical host.

We propose removing the language “Virtual machines hosted on a physical TCA can be treated as software on that physical TCA” from the TCA definition. By removing this language, entities would be required to apply security controls to the virtual machines hosted on their physical TCAs in alignment with CIP-010 R4.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer	No
Document Name	

Comment

The wording for CIP-010 R2.1 is very broad. For example, “changes” could be interpreted multiple ways and should be narrowed down. SPP suggests wording such as: “Security Controls identified in R1.1 should be monitored every 35 days for any unauthorized changes.” Also when the same requirement was applied to R1.1, examples were included in the implementation guidance (e.g., examples of “replacement”).

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

A proposed administrative fixes is: In the Applicable Systems column under “Note:” for Part 1.3 there is an old reference to Part 1.6 that should be updated to Part 1.3.

In Part 3.3 there is confusion over the language being used. The Applicable Systems column references BCS and the Requirements column references both Applicable Systems and Cyber System. The current approved version references Cyber Asset. Can you please clarify if the requirement is for an Applicable System or a Cyber Asset?

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

R3- The concern is that Remediation VLANs should be properly defined in the technical rational or Glossary as it may introduce situations where an entity could inadvertently place production Cyber Assets in this VLAN.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

In CIP-010, Part 2.1, request clarification of the SDT’s intent. Does the new language pertain to 1) version changes in 1.3, 2) changes for CIP-005 & CIP-007 or 3) both?

In CIP-010, Part 3.3, Request clarification on when “Applicable System” starts. Suggest changing the beginning of Requirement from “Prior to becoming a new Applicable System” to “Prior to becoming a new, production Applicable System”

In CIP-010, Attachment 1, 1.3 we recommend removing two bullets because they are not software vulnerability mitigation which is the title of 1.3. The new bullet which is “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution.” The second bullet is “System hardening.” Also, the new bullet preserves the vulnerability which is contrary to good security. The last bullet should remain since it covers alternatives.

In CIP-010, Attachment 1, 1.4 we recommend removing two bullets because they are not mitigating the introduction of malicious code which is the title of 1.4. The new bullet which is “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code.” This new bullet preserves the vulnerability which is contrary to good security. The second bullet is “Application whitelisting;” The last bullet should remain since it covers alternatives.

Since CIP-010, Attachment 2 is the Measures for CIP-010, Attachment 1, we request updates to Attachment 2 per our Attachment 1 comments

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

Per our comments above on R1, NST disagrees with proposed changes that strike references to baselines.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

The new TCA definition includes the use of Virtual Cyber Assets (VCA) as TCAs. This definition is problematic as the definition of a Virtual Cyber Asset includes only logical instances of an operating system or firmware hosted on BCAs, EACMS, PACS, PCAs, or SCI. The Cyber Asset acting as a TCA doesn't fall into any of these categories, so the VCA should not be referenced in the TCA defintion. The new TCA definition implies that each VM on a Cyber Asset is a potential individual TCA.

Likes 0	
Dislikes 0	

Response

Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

R2.1 should address unauthorized changes to CIP-005 and CIP-007 controls. PNMR suggests the following modification to CIP-010 R2.1. “Methods to monitor for unauthorized changes to CIP-005 and CIP-007 controls at least once every 35 calendar days. Document and investigate detected unauthorized changes.”

Likes 0	
Dislikes 0	

Response

Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4

Answer	No
Document Name	

Comment

Tacoma Power is concerned that the scope of change associated to CIP-010-5 R2 part 2.1 is no longer bounded. The current version of CIP-010 R2 Part 2.1 is scoped to only those “changes to baseline configuration (as described in Requirement R1, Part 1.1).”

Tacoma Power suggests the following modification to the proposed language of CIP-010-5 R2 Part 2.1:
“Methods to monitor for unauthorized changes that may impact CIP-005 or CIP-007 security controls (as described in Requirement R1, Part 1.1) at least once every 35 calendar days. Document and investigate detected unauthorized changes.”

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

In CIP-010, Part 2.1, request clarification of the SDT’s intent. Does the new language pertain to 1) version changes in 1.3, 2) changes for CIP-005 & CIP-007 or 3) both?

In CIP-010, Part 3.3, Request clarification on when “Applicable System” starts. Suggest changing the beginning of Requirement from “Prior to becoming a new Applicable System” to “Prior to becoming a new, production Applicable System”

In CIP-010, Attachment 1, 1.3 we recommend removing two bullets because they are not software vulnerability mitigation which is the title of 1.3. The new bullet which is “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution.” The second bullet is “System hardening.” Also, the new bullet preserves the vulnerability which is contrary to good security. The last bullet should remain since it covers alternatives.

In CIP-010, Attachment 1, 1.4 we recommend removing two bullets because they are not mitigating the introduction of malicious code which is the title of 1.4. The new bullet which is “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code.” This new bullet preserves the vulnerability which is contrary to good security. The second bullet is “Application whitelisting;” The last bullet should remain since it covers alternatives. Since CIP-010, Attachment 2 is the Measures for CIP-010, Attachment 1, we request updates to Attachment 2 per our Attachment 1 comments	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy suggests revising the requirement language in CIP-010 R3.3, second bullet, to say “Like replacements **or clone** of the same type of Cyber Systems with a configuration of the previous or existing Cyber System; or ” This revision will include new systems that are added for the same type or clone of a Cyber System.	
Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE suggests revising the requirement language in CIP-010 R3.3, second bullet, to say “Like replacements ***or clone*** of the same type of Cyber Systems with a configuration of the previous or existing Cyber System; or ” This revision will include new systems that are added for the same type or clone of a Cyber System.	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	

Answer	No
Document Name	
Comment	
R2.1 as written broadens beyond the intended scope of requirement R1. LES recommends the following alternative phrasing ‘At least once every 35 calendar days, methods to monitor for changes identified in Requirement R1, Part 1.1 that have not been authorized.’ In addition, LES has concern with the ‘Technical Feasibility’ conforming changes further detailed in the Question 11 response.	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	No
Document Name	
Comment	
The CIP-010-5 Technical Rationale confuses the changes proposed especially around R1. The Technical Rationale includes baselines in R1 and R1 P1.1 that have been removed from the standards. Reference CIP-010-4 Baseline details further complicates and confuses the implementation and does not clearly align with the new CIP-010-5 standard as written. A dormant VM cannot have a baseline run against it that is the same as when it is operating. Yet a VM image file can have a file integrity baseline and then when activated have the operating baselines verified with alerting for deviation and an incident response plan for monitoring deviations.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
CHPD does not agree with the proposed changes to CIP-010. CHPD believes the changes to CIP-010 R1 cause problems to CIP-010 R2.1. A change is fundamentally a difference from what something was previously to what something is now. You fundamentally have to know what something was to tell if it has changed. Knowing the previous state of the system is fundamentally what a baseline configuration is, and that makes it impossible to detect a change without having a baseline configuration. A Responsible Entity might be able to configure events to detect when certain changes occur, but that alert needs to know what the previous state was to know if a change occurred.	

If the SDT wishes to pursue the current language, it will need to either eliminate CIP-010 R2 or rewrite it, as it is not possible to comply with it without tracking a baseline configuration. In keeping with the actual security objective of CIP-010 R1 (ensuring changes do not impact security controls adversely) CHPD recommends looking to TOP-001-4 R21/R24 for guidance. Instead of detecting unauthorized changes, require that RE's perform a test of a subset of CIP-005 and CIP-007 cyber security controls on a periodic basis.

Alternatively, the SDT could keep the baseline configuration requirements, reordering the requirements and removing time frames, and eliminating the proscriptive list of configuration items and allowing Responsible Entities to determine the configuration items for themselves.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Definitions such as SCI is not clear and confusing.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The phrase “prior to becoming a new Applicable System” is confusing and open to multiple interpretations. BPA recommends adding language to clearly scope the Part to the device level.

Prior to adding new applicable Cyber Assets or a new Applicable System, perform an active vulnerability assessment of the new Cyber Assets or Applicable System, except for:

• Like replacements of the same type of Cyber Assets or Applicable Systems with a configuration of the previous or other existing Cyber Assets or Applicable System; or

• CIP Exceptional Circumstances.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

What, if any, impacts will the virtualization modifications have on what is required in a vulnerability assessments that is currently outlined in the Guidelines and Technical Basis?

Also note Attachment 1 was modified starting on page 31 for TCA’s and RM. This seems vague and Attachment 2 doesn’t really help. IE: what is a valid control?

a. “Live operating system and software executable only from read only media” was eliminated. But, in 1.3 “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” was added. Also in 1.4 “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code”

Please provide the technical guidelines within the standard document. We would like more details for what needs to be performed for a VA.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	Yes
Document Name	

Comment

Consider re-writing R2.1 to read, “Methods to monitor at least once every 35 calendar days for changes that were not authorized per Requirement R1. Document and investigate any such detected unauthorized changes.” While potentially minor, this change in language provides more stricture around the term “unauthorized change,” explicitly tying it to the processes established under Requirement R1.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0

Dislikes 0

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

See EEI comment.

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer	Yes
Document Name	

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer	Yes

Document Name

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer Yes

Document Name

Comment

ITC supports the comments submitted by EEI

Likes 0

Dislikes 0

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer Yes

Document Name

Comment

EEI supports the proposed changes.

Likes 0

Dislikes 0

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer Yes

Document Name	
Comment	
Southern supports the revisions to CIP-010.	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Comments: Consider re-writing R2.1 to read, “Methods to monitor at least once every 35 calendar days for changes that were not authorized per Requirement R1. Document and investigate any such detected unauthorized changes.” While potentially minor, this change in language provides more stricture around the term “unauthorized change,” explicitly tying it to the processes established under Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with the proposed changes, but has concerns that the new 1.3 language is less clear. As written, it appears a utility could install new software and not check the source.	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes

Document Name	
Comment	
Patty Ireland on behalf of DTE Energy, Segments 3 and 4	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the proposed changes in CIP-010-5, Requirements R2, R3 and R4.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	
We agree with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	

AZPS agrees that the revisions to CIP-010 helps clarify the risk based approach to change management.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	

All other proposed changes to CIP-010 are acceptable, except for some potential confusion around CIP-010, R4. In R4, the language, “for its high and medium impact BCS and associated PCA *AND* SCI” could be misinterpreted and viewed as all inclusive. NRG proposes to change the AND in “associated PCA *AND* SCI” to OR.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
All other proposed changes to CIP-010 are acceptable, except for some potential confusion around CIP-010, R4. In R4, the language, “for its high and medium impact BCS and associated PCA *AND* SCI” could be misinterpreted and viewed as all inclusive. NRG proposes to change the AND in “associated PCA *AND* SCI” to OR.	
Likes 0	
Dislikes 0	
Response	
Joni Jones - Wabash Valley Power Association - 1	
Answer	Yes
Document Name	
Comment	
no further comments	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	

Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

11. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

CIP-009 R1 does not require a Recovery Plan for SCI, yet CIP-009 R1.5 requires data preservation for SCI during recovery. There is not a mechanism (i.e., a Recovery Plan) in which to document the data preservation requirement if there is Recovery Plan requirement for SCI.

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

CIP-009 R1 does not require a Recovery Plan for SCI, yet CIP-009 R1.5 requires data preservation for SCI during recovery. There is not a mechanism (i.e., a Recovery Plan) in which to document the data preservation requirement if there is Recovery Plan requirement for SCI.

Likes 0	
Dislikes 0	

Response

Mike Marshall - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

The Supplemental Guidelines section of the written standard were helpful in creating applicable controls however with the removal of these technical explanations of new controls should be included with the proposed changes.

Likes 0	
Dislikes 0	

Response	

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Definitions such as SCI is not clear and confusing.

Likes 0	
Dislikes 0	

Response	

Josh Johnson - Lincoln Electric System - 1

Answer	No
Document Name	

Comment

LES recognizes and appreciates the work put into the conforming changes. LES agrees with the vast majority, however, the alternative to the ‘Technical Feasibility Exception (TFE)’ process should incorporate the full range of circumstances currently available to entities. As written, ‘per system capability’ would obligate entities to implement the requirements based solely on whether the Cyber Asset or Cyber System is technically capable whereas the TFE process currently allows entities to apply for exceptions based on operational feasibility, reliability feasibility, resource limitations, safety risks, separate regulatory requirements, and associated costs in addition to the prescribed technical limitations.

LES suggests replacing the phrase 'per system capability' with 'per System Feasibility'. This would require a new term, ‘**System Feasibility**’ which would include the 6 identified circumstances outlined within Appendix 4D of the NERC Rules of Procedure. (Page 2, Section 3.0)

System Feasibility:

Technical or operational circumstances of a Cyber System or Cyber Asset that consider;

- Technical limitations;
- Operational feasibility that could adversely affect reliability of the BES;
- Is technically possible or operationally feasible but has limitations due to scarce technical resources;
- Safety risks or issues that outweigh the benefits of compliance;
- Conflicts with separate statutory or regulatory requirements; or
- Incurrence of costs that far exceed the benefits to the reliability of the BES.

Likes 0	
Dislikes 0	

Response	

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	No
Document Name	

Comment

Manitoba Hydro agrees with the direction of the SDT and all conforming changes to standards CIP-003, CIP-004, CIP-008, CIP-009, CIP-011 and CIP-013. For standard CIP-006 the applicability column does not include SCI. This could create confusion as a VCA designated as an applicable system (BCS for example) would need to be located in a Physical Security Permieter (PSP), however the SCI physically hosting the VCA is not explicitly noted in the applicability column.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

Request clarification of CIP-003 R2. Listing locations containing SCI outside of BES assets is a benefit. However, CIP-003 stipulates that an inventory (list) is not required. How to reconcile these two statements? Should CIP-002 require listing these locations?

Recommend update of CIP-003, Attachment 1, 3.1.i. Recommend new wording and no bullets for improved readability. “Between a low impact BCS or an SCI that supports any part of low BCS and a Cyber System outside the asset containing the low impact BCS(s) or the SCI that supports any part of the Low Impact BCS;"

Recommend update of CIP-003, Attachment 1, 5.1. We recommend removing the new (second) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not “malicious code mitigation” which is the title of Section 5. The new bullet which is “Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code.” The last bullet should remain since it covers alternatives.

Recommend update of CIP-003, Attachment 1, 5.2. We recommend removing the updated (fourth) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not “malicious code mitigation” which is the title of Section 5. The updated bullet which is “Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code.”

If the SDT believes CIP-006 implies physical security of the SCI, we request explicit language in this Standard.

Request correction to CIP-006 Part 1.2 from “Physical Access Control Systems” to “Protected Cyber Assets” for consistency with Part 1.3.

Request update to CIP-008 Part 2.3. For consistency, this Part should include SCI in the Applicable Systems.

Request update to the Parts of CIP-009 R1. If SCI is required for Applicable System recovery, SCI should be included in that recovery plan.

Request clarification on CIP-011 R2 Part 2.1. Is this focus on unauthorized retrieval of BCSI or the lifecycle question of decommissioning of the asset containing BCSI?

Request clarification on CIP-011 R2 Part 2.1. Why is PCA is a Part 2.1 Applicable System but not an Applicable System in Parts 1.1 and 1.2?

We suggest removing R2 to avoid double jeopardy because methods of protection (R1) should include destruction – making R1 sufficient. Plus, R2 is asset based while BCSI is information. This Standard and R1 are focused on information protection

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST agrees with proposed changes to CIP-003, CIP-004, CIP-008, CIP-011, and CIP-013.

NST disagrees with proposed changes to CIP-006 and CIP-009.

CIP-006: NST understands the omission of SCI from any requirement part was intentional, but we disagree with this decision for two reasons. First, it would establish yet more “implied requirements,” as discussed in our comments on Question 1. Second, it is inconsistent with the proposed changes to CIP-004, which would establish explicit requirements to authorize, review and, when appropriate, revoke unescorted physical access to SCI.

CIP-009: NST understands the omission of SCI from any requirement part except for R1.5 (preservation of forensic data if possible) was intentional, but we disagree with this decision, as it would establish yet more “implied requirements,” as discussed in our comments on Question 1. NST acknowledges that in some recovery situations, it might only be necessary to recover a virtual BES Cyber System and not its supporting SCI. However, given the fact the failure or destruction of an SCI could, in some scenarios, wipe out an entire Control Center, NST believes that inclusion of SCI in a Responsible Entity’s recovery plan(s) should be mandatory rather than a suggested best practice.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer	No
Document Name	

Comment

Request clarification of CIP-003 R2. Listing locations containing SCI outside of BES assets is a benefit. However, CIP-003 stipulates that an inventory (list) is not required. How to reconcile these two statements? Should CIP-002 require listing these locations?

Recommend update of CIP-003, Attachment 1, 3.1.i. Recommend new wording and no bullets for improved readability. “Between a low impact BCS or an SCI that supports any part of low BCS and a Cyber System outside the asset containing the low impact BCS(s) or the SCI that supports any part of the Low Impact BCS;"

Recommend update of CIP-003, Attachment 1, 5.1. We recommend removing the new (second) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not “malicious code mitigation” which is the title of Section 5. The new bullet which is “Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code.” The last bullet should remain since it covers alternatives.

Recommend update of CIP-003, Attachment 1, 5.2. We recommend removing the updated (fourth) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not “malicious code mitigation” which is the title of Section 5. The updated bullet which is “Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code.”

If the SDT believes CIP-006 implies physical security of the SCI, we request explicit language in this Standard.

Request correction to CIP-006 Part 1.2 from “Physical Access Control Systems” to “Protected Cyber Assets” for consistency with Part 1.3.

Request update to CIP-008 Part 2.3. For consistency, this Part should include SCI in the Applicable Systems.

Request update to the Parts of CIP-009 R1. If SCI is required for Applicable System recovery, SCI should be included in that recovery plan.

Request clarification on CIP-011 R2 Part 2.1. Is this focus on unauthorized retrieval of BCSI or the lifecycle question of decommissioning of the asset containing BCSI?

Request clarification on CIP-011 R2 Part 2.1. Why is PCA is a Part 2.1 Applicable System but not an Applicable System in Parts 1.1 and 1.2?

We suggest removing R2 to avoid double jeopardy because methods of protection (R1) should include destruction – making R1 sufficient. Plus, R2 is asset based while BCSI is information. This Standard and R1 are focused on information protection

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	No
Document Name	

Comment

CIP-003

- -Attachment 1, Section 2 - How do you control physical access to a VCA? SCI is not required to have protections. Is the expectation that only the specific nodes of the SCI cluster that are hosting the VCA are physically protected?
- Attachment 1, Section 3 – The applicability of requirements to SCI at assets containing low impact BCS is not well defined. CIP-002 does not require the identification of assets containing low impact SCI. If SCI supporting low-impact BCS is spread across multiple assets it is not clear if the protections need to be applied at those other assets as well. For example, some of nodes of an SCI cluster are at a substation and host low impact BCS containing VCAs, but other nodes of that same SCI cluster are located at another asset that does not contain any low impact BCS – it is not clear whether those controls need to be applied there, especially since that asset did not need to be identified in CIP-002.
- Formatting comment only: Attachment 1, Section 3 - the and/or formatting leaves room for confusion - it is not clear that the 'and a Cyber System(s) outside the asset containing:' is not part of the bullet 'An SCI that supports any part of a low BCS', but rather applies to both bullets or'd together.

CIP-006

- Part 1.2 - The applicability column does not include SCI, but does include VCAs (as part of BCS). Scoping the physical requirement to a logical instance could be misleading and allow physical protections to not be applied as necessary. Furthermore, the exclusion of SCI could allow a hypervisor/SCI(1) (hosting non-CIP VCA) that's part of the SCI cluster which is geographically dispersed from the SCI(2) hosting a BCS. The requirement infers that as soon as the SCI(1) hosts an applicable CIP VCA it would require PSP protections. But if the SCI(1) is not hosting an applicable system in CIP-006 R1.2 it would not require PSP protections. An alternate approach would be to include SCI as an applicable system.

- Part 1.3 – The change from "where technically feasible" to "per system capability" removes the requirement for mitigation of the risks posed by the feasibility exception. The requirement is not prescriptive to specific technical controls, this provides flexibility that should not be limited to technical infeasibility. For a PSP protecting high impact BCS, it seems unreasonable to allow for implementations that aren't capable of using two or more physical access controls without mitigation of the risk.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

In CIP-003, concerned about the amibigous language of "supports any part of the low impact BCS" and what exactly that means. This makes sense for SCI that directly supports a BROS function of the low impact BCS, but "[supporting] any part" may lead to misinterpretations. For example, does "support" include:

- Security controls an entity implements that are above and beyond the CIP-003 standards? e.g if an entity implements a virtualized configuration monitoring tool specific for low impact in their Data Center and it scans remote low impact BCS, am I required per CIP-003 to control inbound/outbound permissions or utilize a TCA program to the security tool SCI in the DC that otherwise doesn't fall under CIP scope?

- Operational tools an entity uses to run/manage the low impact BCS? E.g. if an entity implements a virtualized system monitoring tool that identifies system health (e.g. up/down status, processor utilization, memory utilization, bandwidth, etc) of the low impact BCS in their Data Center, am I required per CIP-003 to control inbound/outbound permissions or utilize a TCA program to the health monitoring SCI in the DC that otherwise doesn’t fall under CIP scope?

- Data aggregation tools that collect data not used in a real-time horizon as defined by NERC? E.g if an entity implements a data aggregation tool that collects system that is not used for real-time decision making or any other real-time horizon, but helps “support” the operation of the low impact BCS (e.g. configurations, set-points, fault tracking, historian, etc) in their Data Center, am I required per CIP-003 to control inbound/outbound permissions or utilize a TCA program to the data aggregation tool SCI in the DC that otherwise doesn’t fall under CIP scope?

Concerned the ambiguous definition of “support” may bring assets/tools/SCI into scope that otherwise would not be. Recommend more descriptive language or a definition of “support” to ensure the proper scope is obtained.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes. Further, introducing Shared Cyber Infrastructure (SCI) increases the number of Requirements and Parts that a Responsible Entity needs to track compared to simply identifying the hypervisor and associated hardware and “high-water marking” them with the highest identified impact rating BCA/VCA and creating a BCS.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer	No
Document Name	

Comment

Except for the comments regarding the definitions for VCA, SCI, EAP, PCA, and ERC as noted above in Question 1-6, SPP supports the changes the SDT has made to the Requirements for CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.

If the SDT continues with another version of the standards, SPP suggests the SDT consider the following actions or clarifications:

- Should SCI be included as part of R1.1 for CIP-009?

- For CIP-008 R4,. add "…, or their successors" in the R4 requirement of the language after Cybersecurity & Infrastructure Security Agency (CISA).

Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
IESO supports the comments provided by NPCC and IRC	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	

CIP-003 – *No, we have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard.*

CIP-004 – No, we have concerns with the SCI and IRS definitions. These terms are used throughout the Standard.

CIP-006 – Yes

CIP-008 – No, we have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard.

CIP-009 - No, we have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard.

CIP-011 - No, we have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard.

CIP-013 - No, we have concerns with the SCI definition and it potentially bringing additional devices into scope. This term is used throughout the Standard.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request clarification of CIP-003 R2. Listing locations containing SCI outside of BES assets is a benefit. However, CIP-003 stipulates that an inventory (list) is not required. How do you reconcile these two statements? Should CIP-002 require listing these locations?

Recommend update of CIP-003, Attachment 1, 3.1.i. Recommend new wording and no bullets for improved readability. “Between a low impact BCS or an SCI that supports any part of low BCS and a Cyber System outside the asset containing the low impact BCS(s) or the SCI that supports any part of the Low Impact BCS;"

Recommend update of CIP-003, Attachment 1, 5.1. We recommend removing the new (second) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3, and 1.4. We recommend removing the new bullet because it is not “malicious code mitigation” which is the title of Section 5. The new bullet is “Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code.” The last bullet should remain since it covers alternatives.

Recommend update of CIP-003, Attachment 1, 5.2. We recommend removing the updated (fourth) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3, and 1.4. We recommend removing the new bullet because it is not “malicious code mitigation” which is the title of Section 5. The updated bullet is a “Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code.”

If the SDT believes CIP-006 implies the physical security of the SCI, we request explicit language in this Standard.

Request correction to CIP-006 Part 1.2 from “Physical Access Control Systems” to “Protected Cyber Assets” for consistency with Part 1.3.

Request update to CIP-008 Part 2.3. For consistency, this Part should include SCI in the Applicable Systems.

Request update to the Parts of CIP-009 R1. If SCI is required for Applicable System recovery, SCI should be included in that recovery plan.

Request clarification on CIP-011 R2 Part 2.1. Is this focus on unauthorized retrieval of BCSI or the lifecycle question of decommissioning the asset containing BCSI?

Request clarification on CIP-011 R2 Part 2.1. Why is PCA a Part 2.1 Applicable System but not an Applicable System in Parts 1.1 and 1.2?

We suggest removing R2 to avoid double jeopardy because methods of protection (R1) should include destruction – making R1 sufficient. Plus, R2 is asset-based while BCSI is information. This Standard and R1 are focused on information protection.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

We support NPCC TFIST comments.

Request clarification of CIP-003 R2. Listing locations containing SCI outside of BES assets is a benefit. However, CIP-003 stipulates that an inventory (list) is not required. How to reconcile these two statements? Should CIP-002 require listing these locations?

Recommend update of CIP-003, Attachment 1, 3.1.i. Recommend new wording and no bullets for improved readability. “Between a low impact BCS or an SCI that supports any part of low BCS and a Cyber System outside the asset containing the low impact BCS(s) or the SCI that supports any part of the Low Impact BCS;"

Recommend update of CIP-003, Attachment 1, 5.1. We recommend removing the new (second) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not “malicious code mitigation” which is the title of Section 5. The new bullet which is “Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code.” The last bullet should remain since it covers alternatives.

Recommend update of CIP-003, Attachment 1, 5.2. We recommend removing the updated (fourth) bullet which is consistent with our comments on CIP-010, Attachment 1, 1.3 and 1.4. We recommend removing the new bullet because it is not “malicious code mitigation” which is the title of Section 5. The updated bullet which is “Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code.”

If the SDT believes CIP-006 implies physical security of the SCI, we request explicit language in this Standard.

Request correction to CIP-006 Part 1.2 from “Physical Access Control Systems” to “Protected Cyber Assets” for consistency with Part 1.3.

Request update to CIP-008 Part 2.3. For consistency, this Part should include SCI in the Applicable Systems.

Request update to the Parts of CIP-009 R1. If SCI is required for Applicable System recovery, SCI should be included in that recovery plan.

Request clarification on CIP-011 R2 Part 2.1. Is this focus on unauthorized retrieval of BCSI or the lifecycle question of decommissioning of the asset containing BCSI?

Request clarification on CIP-011 R2 Part 2.1. Why is PCA is a Part 2.1 Applicable System but not an Applicable System in Parts 1.1 and 1.2?

We suggest removing R2 to avoid double jeopardy because methods of protection (R1) should include destruction – making R1 sufficient. Plus, R2 is asset based while BCSI is information. This Standard and R1 are focused on information protection

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	
Comment	

Suggest adding SCI to the Note for CIP-003 R2

Request clarification of CIP-003 R2. Listing locations containing SCI outside of BES assets is a benefit. However, CIP-003 stipulates that an inventory (list) is not required. How to reconcile these two statements? Should CIP-002 require listing these locations?

If the SDT believes CIP-006 implies physical security of the SCI, we request explicit language in this Standard.

Request update to CIP-008 Part 2.3. For consistency, this Part should include SCI in the Applicable Systems.

Request update to the Parts of CIP-009 R1. If SCI is required for Applicable System recovery, SCI should be included in that recovery plan.

Request clarification on CIP-011 R2 Part 2.1. Why is PCA a Part 2.1 Applicable System but not an Applicable System in Parts 1.1 and 1.2?

We suggest removing R2 to avoid double jeopardy because methods of protection (R1) should include destruction – making R1 sufficient. Plus, R2 is asset based while BCSI is information. This Standard and R1 are focused on information protection

Likes 0	
Dislikes 0	
Response	

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Scott Miller

Answer	No
Document Name	
Comment	

RE: CIP-003

o The addition of controls for low impact in Attachment 1 Section 5 are the same/similar to the addition of controls for high/medium impact in CIP-010 Attachment 1, Section 1. This addition for low impact is overly burdensome and would stretch the resources of companies that have a significant number of low impact assets, with a minimal increase in the security/protection of the BES. While low impact should be protected, the protection should be appropriate for the impact rating to the BES and not on the same level as high/medium impact.

Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring

Answer	Yes
Document Name	
Comment	
WECC supports the revisions but has one question for consideration. Considering SCI is included in the applicability table of CIP-009-7 R1 Part 1.5. Was it the intent of the SDT to exclude SCI from other requirements? Specifically, this exclusion appears to not require a PSP or ESP for SCI.	
Likes 0	
Dislikes 0	
Response	
Joni Jones - Wabash Valley Power Association - 1	
Answer	Yes
Document Name	
Comment	
no further comments	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	

Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE suggests the language “except during CIP Exceptional Circumstances” in CIP-006 Part 2.2 can be removed as it is part of the parent Requirement R2 and thus applies to all parts.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes to the additional CIP standards contained within Project 2016-02.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	

Comment	
We agree with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE agrees with the conforming changes to the remaining requirements.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the proposed changes in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013. AEP also suggests minor edit by adding the word "*are*" in Attachment 2 to CIP-003-Y, Section 3, item 1, "…. that the Responsible Entity deems necessary, except where an entity provides rationale that communications ***are*** between Protection Systems."	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	

SDG&E supports EEI's comments:

CIP-003 – EEI supports the proposed changes made to CIP-003. (Note the proposed change to Attachment 1 was incorporated into the standard.)

CIP-004 – EEI supports the proposed changes made to CIP-004.

CIP-006 – EEI supports the proposed changes made to CIP-006

CIP-008 – EEI supports the proposed changes made to CIP-008, however, the phrase “SCI supporting an Applicable System in this Part” is missing from Requirement R2, subpart 2.3.

CIP-009 – EEI supports the proposed changes made to CIP-009.

CIP-011 – EEI supports the proposed changes made in CIP-011.

CIP-013 – EEI supports the proposed changes made in CIP-013.

Likes 0	
Dislikes 0	

Response

patricia ireland - DTE Energy - 4

Answer	Yes
Document Name	

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 0	
Dislikes 0	

Response

Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon

Answer	Yes
Document Name	

Comment

It would be helpful with large scale changes such as this to be able to see an example/draft of the new ERT that could be released to track the new information required.

Likes 0	

Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Comments: We agree with limiting the changes in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 to only what is needed to conform with the changes in CIP-005, CIP-007, and CIP-010. We believe this is a far more efficient and implementable approach.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the changes made to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

CIP-003 – EEI supports the proposed changes made to CIP-003. (Note the proposed change to Attachment 1 was incorporated into the standard.)

CIP-004 – EEI supports the proposed changes made to CIP-004.

CIP-006 – EEI supports the proposed changes made to CIP-006

CIP-008 – EEI supports the proposed changes made to CIP-008, however, the phrase “SCI supporting an Applicable System in this Part” is missing from Requirement R2, subpart 2.3.

CIP-009 – EEI supports the proposed changes made to CIP-009.

CIP-011 – EEI supports the proposed changes made in CIP-011.

CIP-013 – EEI supports the proposed changes made in CIP-013.

Likes 0	
Dislikes 0	

Response

John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1

Answer	Yes
Document Name	

Comment

Tacoma Power suggests reinstating a modified version of CIP-006 R1 Part 1.10 to exclude the Super ESP concepts, referring to one geographical location work with the Exemption 4.2.3.3 language.

Suggested CIP-006 R1.10 modification:

“Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same geographic location and Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.”

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
The current draft is significantly more digestable than previous drafts by limiting changes to the other less technical standards and fits today's current configurations while allowing flexibility for new and future technologies.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)	
Answer	Yes
Document Name	
Comment	
The SRC does not have concern with these proposed conforming changes and agrees with them. *SPP did not participate in this response.*	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	

Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
See EEI comment.	

Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
AEPCO is signing on to ACES comments below. ACES Comments: The current draft is significantly more digestable than previous drafts by limiting changes to the other less technical standards and fits today’s current configurations while allowing flexibility for new and future technologies.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones	
Answer	Yes
Document Name	
Comment	
We agree with limiting the changes in CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 to only what is needed to conform with the changes in CIP-005, CIP-007, and CIP-010. We believe this is a far more efficient and implementable approach.	

Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	

Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	

12. The SDT has revised numerous VSL's for simplification. Do you agree with the proposed changes? If not, please provide the basis for your disagreement.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We agree with the approach to simplify the VSLs. However, some updates are needed.

CIP-003: lower VSL, R2 – delete "but" (The Responsible Entity but failed to manage its Transient Cyber Asset(s)…"

CIP-004: For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, "The Responsible Entity did not authorize electronic access or unescorted physical access based on need for" one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004 access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.

Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidently granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that's a different matter entirely.

For CIP-004 R6, the last item in moderate VSL is missing "not."

CIP-005: R1.3 severe VSL needs "per cyber asset capability" added. The reference to "method to protect data traversing" item should be Part 1.4, not Part 1.3.

CIP-007 R4.3 high VSL needs to have "per cyber asset capability" added.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	No
Document Name	

Comment

We are in agreement with NSRFs comments regarding VSLs.

Likes 0	

Dislikes 0

Response

Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3

Answer No

Document Name

Comment

CIP-010-5 R1 VSL, the first violation under Moderate VSL and High VSL are worded exactly the same. In CIP-010-4 the difference is leaving out 3/5 baseline elements vs 2/5 baseline elements. Without this quantitative distinction, it is difficult to determine VLS for potential non-compliance.

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer No

Document Name

Comment

We agree with the approach to simplify the VSLs. However, some updates are needed.

- CIP-003: lower VSL, R2 – delete “but” (The Responsible Entity but failed to manage its Transient Cyber Asset(s)…”
- CIP-004: For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, “The Responsible Entity did not authorize electronic access or unescorted physical access based on need for” one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004 access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.
- Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidently granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that’s a different matter entirely.
- For CIP-004 R6, the last item in moderate VSL is missing “not.”
- CIP-005: R1.3 severe VSL needs “per cyber asset capability” added. The reference to “method to protect data traversing” item should be Part 1.4, not Part 1.3.
- CIP-007 R4.3 high VSL needs to have “per cyber asset capability” added.

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer	No
Document Name	

Comment

We agree with the approach to simplify the VSLs. However, some updates are needed.

CIP-003: lower VSL, R2 – delete “but” (The Responsible Entity but failed to manage its Transient Cyber Asset(s)…”

CIP-004: For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, “The Responsible Entity did not authorize electronic access or unescorted physical access based on need for” one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004 access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.

Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidently granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that’s a different matter entirely.

For CIP-004 R6, the last item in moderate VSL is missing “not.”

CIP-005: R1.3 severe VSL needs “per cyber asset capability” added. The reference to “method to protect data traversing” item should be Part 1.4, not Part 1.3.

CIP-007 R4.3 high VSL needs to have “per cyber asset capability” added.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

We agree with the approach to simplify the VSLs. However, some updates are needed.

CIP-003: lower VSL, R2 – delete “but” (The Responsible Entity but failed to manage its Transient Cyber Asset(s)…”

CIP-004: For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, “The Responsible Entity did not authorize electronic access or unescorted physical access based on need for” one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004 access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.

Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidently granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that's a different matter entirely.

For CIP-004 R6, the last item in moderate VSL is missing "not."

CIP-005: R1.3 severe VSL needs "per cyber asset capability" added. The reference to "method to protect data traversing" item should be Part 1.4, not Part 1.3.

CIP-007 R4.3 high VSL needs to have "per cyber asset capability" added.

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	Yes
Document Name	

Comment

We largely agree with the proposed changes but also urge the following changes.

For CIP-003: lower VSL, R2 – delete the word "but" (The Responsible Entity but failed to manage its Transient Cyber Asset(s)…"

For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, "The Responsible Entity did not authorize electronic access or unescorted physical access based on need for" one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004 access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.

Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidently granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that's a different matter entirely.

For CIP-005, the R1.3 severe VSL should have "per system capability" added. The reference to "method to protect data traversing" item should be Part 1.4, not Part 1.3.

For CIP-007, the R4.3 high VSL should have "per system capability" added.

Likes 0	

Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Alliant Energy supports the comments submitted by the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

See EEI comment.

Likes 0	
Dislikes 0	

Response

Alison Mackellar - Constellation - 5

Answer	Yes
Document Name	

Comment

Constellation has elected to align with Exelon in response to this question.

Kim Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We agree with the new language. It is easier to read when VSLs explain what should have been done (per Requirements) but was not done.	

Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the proposed revisions to the VSLs.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	Yes
Document Name	
Comment	
We support NPCC TFIST comments.. We agree with the new language. It is easier to read when VSLs explain what should have been done (per Requirements) but was not done.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
We agree with the new language. It is easier to read when VSLs explain what should have been done (per Requirements) but was not done.	
Likes 0	

Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
IESO supports the comments provided by NPCC and IRC	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the changes to the VSLs.	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer Yes

Document Name

Comment

Comments: We largely agree with the proposed changes but also urge the following changes.

For CIP-003: lower VSL, R2 – delete the word “but” (The Responsible Entity but failed to manage its Transient Cyber Asset(s)…”

For CIP-004, the SDT is proposing adding new VSLs for R4.1. The suggested additions read, “The Responsible Entity did not authorize electronic access or unescorted physical access based on need for” one, two, etc. individuals. We think the intent here is that Responsible Entities are out of compliance if they provide electronic or unescorted physical access without properly processing the individual(s) through the established CIP-004 access management program. The added VSLs as written, however, imply the opposite, that a Responsible Entity is out of compliance if they ever refuse access. We urge the SDT to clarify the wording of these VSLs.

Further on CIP-004 VSLs for R4.1, the VSLs should begin under the Lower category (not Moderate), and the SDT should consider revising how many individuals are in each category (ex. one to two for Lower, three to five for Moderate, six to nine for High, anything over that for Severe). Alternatively, rather than classify the VSL by number of individuals, perhaps it should instead be based on length of time that the violation occurred. If 10 individuals are accidentally granted unescorted physical access but only for an hour or less, that may not be a severe risk. If a single individual has erroneously had electronic access for over a year, that’s a different matter entirely.

For CIP-005, the R1.3 severe VSL should have “per system capability” added. The reference to “method to protect data traversing” item should be Part 1.4, not Part 1.3.

For CIP-007, the R4.3 high VSL should have “per system capability” added.

Likes 0

Dislikes 0

Response

Carl Pineault - Hydro-Qu?bec Production - 5

Answer Yes

Document Name

Comment

We agree with the new language. It is easier to read when VSLs explain what should have been done (per Requirements) but was not done.

Likes 0

Dislikes 0

Response

patricia ireland - DTE Energy - 4

Answer	Yes
Document Name	

Comment

Patty Ireland on behalf of DTE Energy, Segments 3 and 4

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	Yes
Document Name	

Comment

We agree with the new language. It is easier to read when VSLs explain what should have been done (per Requirements) but was not done.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CEHE agrees with the approach to simplify the VSL’s.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer	Yes

Document Name	
Comment	
We agree with the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes to the VSLs.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	

Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response
David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response
Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response
Glen Farmer - Avista - Avista Corporation - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	

Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST has no comment.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment	
Texas RE noticed CIP-005 is missing VSLs for CIP-005 R1.4.	
Likes 0	
Dislikes 0	
Response	

13. The SDT has revised the Implementation Plan to include the Planned and Unplanned Changes provisions and to allow for early adoption. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

Time frames to implement seem to be rather constrained. Propose 36 months.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	No
Document Name	

Comment

- NEE is requesting the implementation period be extended to 36-months. Supply chain risks including parts and staffing availability impact the implementation especially for large entities required to support multiple locations, divergent technologies and large geographical areas spanning multiple NERC regions. Managing the tiered implementation creates risk for enterprise based procedures and training spanning multiple NERC registrations supporting all the impact ratings applicable to the updated NERC CIP standards.
- Currently implemented technology limitations prevent compliance in some instances requiring complex projects coordinated with multiple vendors and suppliers which are estimated to take at minimum 24-months, for example to address the SCI shared memory and CPU requirements. Replacement of capital hardware and depreciation can have adverse economic costs for Cyber Assets approved in rate cases and on existing financial depreciation schedules.
- Another recommendation worthy of consideration would allow for grandfathering of some equipment out to 36 or 46 months for replacement of equipment to apply the new definitions and requirements.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP recommends adding a time frame for the planned changes to account for planned changes that may not have enough lead time because of last minute changes. Therefore, AEP recommends modifying the first sentence as follows, “Planned changes, **further out than 12-month**, refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.” And for the unplanned changes, AEP recommends adding transfer of ownership as an unplanned change and add it to the “Scenario of Unplanned Changes After the Effective Date” table of the implementation plan with a 24-month compliance implementation.

Likes 0

Dislikes 0

Response

Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

Although we agree with the option of early adoption, PNMR recommends extending the implementation. Highly complex and wholesale changes across all standards creates significant burden to utilities. Just the learning curve to fully understand the standards may be excessive. Expertise and resource availability adds additional risk to compliance. This requires a paradigm shift in security and compliance management. We would expect significant and ongoing outreach and training. Due to the complexity, PNMR would recommend 36 month implementation timeline.

Likes 0

Dislikes 0

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley

Answer	No
Document Name	

Comment

Given the number and extend of the changes to the Reliability Standards to support virtualization, the time and cost to budget for and purchase additional equipment, and because there could be significant architectural changes to an entity’s network infrastructure, SMUD would propose a longer implementation plan of 36-months. This would ensure that entities have proper time to design, fund, implement, document, and adjust training associated with the proposed changes. A 24-month implementation might work for entities that need to make only minor adjustments, but 24 months could be difficult to meet for entities that are currently co-mingling SCI resources on a much larger scale.

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
We question if 12 months is sufficient when the entity has a significant increase in High or Medium Impact.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question.	

Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joni Jones - Wabash Valley Power Association - 1	
Answer	Yes
Document Name	
Comment	
no further comments	
Likes 0	
Dislikes 0	
Response	
George Brown - Acciona Energy North America - 5	
Answer	Yes
Document Name	
Comment	
Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.	
Likes 0	

Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with he proposed Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF	
Answer	Yes
Document Name	
Comment	
We agree with the proposed changes.	
Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE agrees with the revised implementation plan.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Generally, we agree with the revised Implementation Plan but request the SDT consider if 12 months is sufficient when the entity has a significant increase (change) in High or Medium Impact Level.	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4	
Answer	Yes
Document Name	
Comment	
Patty Ireland on behalf of DTE Energy, Segments 3 and 4	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Generally, we agree with the revised Implementation Plan but request the SDT consider if 12 months is sufficient when the entity has a significant increase (change) in High or Medium Impact Level.	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
This is related to unplanned changes to asset classifications, not unplanned (Emergency) changes, thus no issues for IT Change Management (PEB)	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	Yes

Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the revised Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
IESO supports the comments provided by NPCC and IRC	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	

Generally, we agree with the revised Implementation Plan but request the SDT consider if 12 months is sufficient when the entity has a significant increase (change) in High or Medium Impact Level.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	Yes
Document Name	

Comment

We support NPCC TFIST comments.

Generally, we agree with the revised Implementation Plan but request the SDT consider if 12 months is sufficient when the entity has a significant increase (change) in High or Medium Impact Level.

Likes 0

Dislikes 0

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the proposed Implementation Plan.

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 3)

Answer	Yes
Document Name	

Comment

The SRC does not have concern with the revised Implementation Plan and agrees with the proposed change.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
See EEI comment.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Quintin Lee - Eversource Energy - 1, Group Name Eversource Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Marshall - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Strom - Buckeye Power, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Johnson - Lincoln Electric System - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bridget Silvia - Sempra - San Diego Gas and Electric - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hien Ho - Tacoma Public Utilities (Tacoma, WA) - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Allen Klassen, Evergy, 6, 1, 3, 5; Derek Brown, Evergy, 6, 1, 3, 5; Marcus Moor, Evergy, 6, 1, 3, 5; Thomas ROBBEN, Evergy, 6, 1, 3, 5; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC, Group Name SPP RTO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Merrell - Tacoma Public Utilities (Tacoma, WA) - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Barry Jones - Barry Jones On Behalf of: sean erickson, Western Area Power Administration, 1, 6; - Barry Jones

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE is concerned there is conflicting language in the planned changes section of the implementation plan, as well as language in the unplanned changes section in the proposed implementation plan that could result in a reliability gap.

Regarding the conflicting language addressing planned changes, Texas RE notes that the second paragraph in the proposed implementation plan states: “For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.”

Texas RE understands this language to mean the BCS at the substation must be compliant upon the commissioning of the substation. Texas RE agrees with this position.

However, the first and third paragraphs in the proposed implementation plan appears to conflict with this reading. Specifically, the first paragraph states: “Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.” Furthermore, the proposed implementation plan’s third paragraph states: “For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan."

Texas RE understands this language to mean the BCS at the substation is not required to be compliant until the Registered Entity has performed its annual assessment under CIP-002 R2. This introduces a reliability gap as assets that were commissioned shortly after the entity has completed a CIP-002 R2 evaluation will not be required to be evaluated for up to 15 calendar months, and therefore would not be required to be compliant with the applicable cyber security requirements. Texas RE does not agree with this position. Additionally, there are no requirements to identify PACS, EACMS, or PCAs.

Regarding the proposed implementation plan's concerning unplanned changes, Texas RE is concerned the language could be read to result in a reliability gap. Specifically, the first paragraph of the implementation plan states "Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2."

Texas RE notes that while it is true that during a CIP-002 R2 review an entity may discover that a BCS now meets a higher BCS threshold than it previously held, this is not the only situation in which an entity may become aware of the need for a higher categorization. For example, if an entity is informed by their RC, PC, or TP that an asset is critical to the derivation of an IROL then the knowledge that the systems must meet the medium impact criteria is immediate and as such the 12-month timer to implement medium impact controls should begin immediately. As written, the language in the implementation plan could result in a situation where a Registered Entity could delay the implementation of medium impact controls at such a substation or power plant for up to 27 calendar months, if the IROL notification arrived immediately after a CIP-002 R2 evaluation. Texas RE recommends the SDT revise the proposed implementation plan language around "unplanned changes" to preclude this result.

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon would like the Standard Drafting Team to consider a 36-month implementation plan prior to enforcement.

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer	
Document Name	
Comment	
Exelon would like the Standard Drafting Team to consider a 36-month implementation plan prior to enforcement.	
Likes 0	
Dislikes 0	
Response	

14. Please provide any additional comments for the drafting team to consider, if desired.

David Rudolph - Basin Electric Power Cooperative - 1	
Answer	
Document Name	
Comment	
By eliminating the language for BCSI repositories, complying with the new CIP-004_R6 will be nearly impossible.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
Thank you for the opportunity to provide feedback.	
Likes 0	
Dislikes 0	
Response	

Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	
Constellation has elected to align with Exelon in response to this question. Kim Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	
Document Name	
Comment	
ITC has received this comment from one of our departments: As far as the implantation plan.. I'd like some more clarity that the 'upon commission' language has been removed from planned changes and the CIP standards only apply to impacted planned changes upon completion of the next annual assessment.	
Likes 0	
Dislikes 0	
Response	

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
There is inconsistent capatilization of Applicable Systems (CIP-005 R3.2, CIP-013 VSL)	
Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	
Document Name	

Comment

We would like to thank the Project 2016-02 SDT on their hard work, dedication, and continuing to listen to industry feedback to meet the FERC order and not create significantly more compliance burden.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley

Answer	
Document Name	

Comment

· In some Reliability Standards, acronyms are used prior to expanding them at first use (e.g. VCA, SCI, etc.).

· In some cases acronyms are expanded (e.g. EACMS and PACS) and other times the acronyms are used (e.g. BCS, TCA).

· Sometime the term BCS is used and other times the term BCA is used (especially around device capability)

· Moving some of the requirement language in the existing Reliability Standards to the "measures" section of the proposed new Standards is confusing (e.g. specifically CIP-010 R1.1). It's unclear what security controls from CIP-005 and CIP-007 are supposed to be tracked in the new requirement. Only in the measures section does it mention anything about elements to monitor, however, none of those items exist in CIP-005 or CIP-007. This makes the controls vague because the details are no longer in CIP-005 and CIP-007.

· The current wording in CIP-010 is preferred over the proposed language.

· There are changes to requirements that do not seem to directly support virtualization technologies. The focus should be putting SCI and Management Interfaces in the applicability sections and only changing the requirements where necessary to support virtualization (e.g. CIP-005).

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer

Document Name

Comment

We compliment the standard drafting team on great progress at addressing industry comments submitted during the last posting. While we are providing few comments on the standards themselves, we believe some changes are needed to several definitions. Since there is no ballot for the definitions alone, we will be voting negative on CIP-005, the standard that we think is most affected by issues with the definitions.

We request that NERC propose consolidation of the effective dates for CIP-004-7 and CIP-011-3 with the effective dates of this project. This would reduce the administrative burden of having to implement multiple versions for these two standards within a short time period.

Likes 0

Dislikes 0

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer

Document Name

Comment

EEI would like to convey our sincere appreciation to the Project 2016-02 Standards Drafting Team for their diligent efforts and dedication to excellence throughout this long and difficult project. We would also like to assure all of you that your efforts and hard work have not gone unnoticed by EEI and the industry broadly. Many thanks to all of you!

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon will align with EEI in response to this question.

Likes 0

Dislikes 0

Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon will align with EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
No additional comment	
Likes 0	
Dislikes 0	
Response	
Maggy Powell - Amazon Web Services - 7	
Answer	
Document Name	
Comment	
The SDT is clear that this project SAR focuses on on-premise virtualization, however, many virtualization concepts convey use of cloud. AWS suggests explicitly stating whether these new terms/requirements, specifically SCI, will apply to cloud or not. If these terms/requirements do not apply to cloud, it should be obvious to the reader.	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	
Document Name	

Comment

Tri-State appreciates the hard work the drafting team did to incorporate industry feedback into this project.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	
Document Name	

Comment

Conflating support for both High-, Medium-, and Low-Impact Cyber Assets within a single Virtualization Cluster could create confusion. Clusters by their very nature include pools of shared SCI to include CPU, Memory, Disk, and network resources that are shared between all Cluster members to allow for balancing resources, recovery from failed hardware, and maintaining high availability. The complexity required to balance these pooled resources and disallow different impact levels of VM guests from running on the same physical resources could be high. Moving VM guests can take place without the need for clustering and would allow for segregated siloing of different impact Cyber Assets without the requirement of determining high-water marking every time a VM guest is moved. Communications play a key role in determining the current health and configuration of clusters – especially with heartbeats and SCSI data requests. Responsible Entities have a high bar to assure that these communications are not to the point that they create common networking connections that would start to include additional VM Guests as PCA.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	
Document Name	

Comment

We compliment the Project 2016-02 Standard Drafting Team on being receptive to industry feedback, to rethinking past proposed revisions, and to proposing a path forward that we believe is as efficient and implementable as possible for allowing for technologies to be utilized for critical infrastructure protection.

Regarding the lack of a separate ballot for the definitions, we believe this is an oversight that needs to be corrected. The definitions are crucially important, particularly in this project. If not corrected, we request action by NERC to ensure that in future this circumstance does not recur.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	
No additional comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	
Document Name	
Comment	
NST has no further comments.	
Likes 0	
Dislikes 0	
Response	
Jennifer Malon - Jennifer Malon On Behalf of: Brooke Voorhees, Black Hills Corporation, 3, 5, 1, 6; Derek Silbaugh, Black Hills Corporation, 3, 5, 1, 6; Don Stahl, Black Hills Corporation, 3, 5, 1, 6; Seth Nelson, Black Hills Corporation, 3, 5, 1, 6; - Jennifer Malon	
Answer	
Document Name	
Comment	

When large changes that add and remove requirements are performed on a standard we feel it would be very helpful to not re-use existing requirement numbers for very different requirements. For example CIP-005 has a large number of requirement numbers that drastically change the intent and requirement between the new and old versions. We fear that this could lead to confusion and potential for errors as both human memory and systems built to monitor specific requirements struggle to adapt to the drastic change in intent.

Likes 0

Dislikes 0

Response

Donald Lock - Talen Generation, LLC - 5

Answer

Document Name

Comment

The sea change being attempted in NERC’s CIP definitions makes the success of the vitualization initiative highly dependent on clear communications, making significantly expanded explanations (with examples) appropriate, including clarifying that the new term, “Shared Cyber Infrastructure,” applies to hypervisors and not GO-TO communications systems

Likes 0

Dislikes 0

Response

Dwanique Spiller - Dwanique Spiller On Behalf of: Kevin Salsbury, Berkshire Hathaway - NV Energy, 5; - Berkshire Hathaway - NV Energy - 5 - WECC

Answer

Document Name

Comment

We compliment the standard drafting team on great progress at addressing industry comments submitted during the last posting. While we are providing few comments on the standards themselves, we believe some changes are needed to several definitions. Since there is no ballot for the definitions alone, we will be voting negative on CIP-005, the standard that we think is most affected by issues with the definitions.

We request that NERC propose consolidation of the effective dates for CIP-004-7 and CIP-011-3 with the effective dates of this project. This would reduce the administrative burden of having to implement multiple versions for these two standards within a short time period.

Likes 0

Dislikes 0

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer

Document Name

Comment

N/A

Likes 0

Dislikes 0

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer

Document Name

Comment

CEHE believes requirements CIP-008 R3 and CIP-009 R3 are administrative in nature and do not add to reliability or security. Sub-requirements in R3 around 90-day and 60-day notifications have been more of an administrative burden than a reliability benefit. The parent requirement of having a plan and executing the plan every 15 calendar months should suffice. CEHE recommends the SDT re-evaluate these requirements for potential revision or retirement.

Likes 0

Dislikes 0

Response

Bryan Koyle - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer

Document Name

Comment

SIGE believes requirements CIP-008 R3 and CIP-009 R3 are administrative in nature and do not add to reliability or security. Sub-requirements in R3 around 90-day and 60-day notifications have been more of an administrative burden than a reliability benefit. The parent requirement of having a plan and executing the plan every 15 calendar months should suffice. CenterPoint Energy recommends the SDT re-evaluate these requirements for potential revision or retirement.

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - SERC,RF

Answer	
Document Name	

Comment

We would like to thank the SDT for their hard work producing this draft. Duke Energy has no additional comments.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	
Document Name	

Comment

- CIP-002-7 Please update Technical Rationale and Justification for Reliability Standard replacing CIP-002-5.1 with CIP-002-7 in the Table of Contents and other references such as Appendix 1
- Please add references and application to Technical Rationale and Justification for Reliability Standard for the new SCI, VCA, CS, MI.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	
Document Name	

Comment

Reclamation recommends that improved resilience or reliability of the BES should be the primary consideration before an entity adopts any new or emerging technologies for BES reliability operating services.

Reclamation identifies that in the drafts for CIP-005 and CIP-010, the drafting team has inserted new requirements in the existing numbering structure (shifting subsequent numbers by +1). So, if the requirement was R3, and a new requirement was inserted before, R3 would now become R4 and so on. Or if a requirement was removed, the subsequent numbers are decreased accordingly. O&P standard drafting teams have deployed a method to mark deleted requirement numbers as "Reserved" to maintain the consistency of the number sequence. Reclamation recommends this practice be adopted for CIP standards and also recommends that if new requirements are added, they should be added at the end of the existing requirements to preserve the existing v5 number sequence. If new requirements are added after a space in the sequence has opened, they can be inserted without changing the rest of the numbering.

Reclamation also recommends utilizing existing FedRAMP criteria and air gapping Industrial Control Systems from external communications where possible.

Reclamation appreciates the SDT’s efforts to incorporate the NIST Framework into the NERC standards. Reclamation encourages the SDT to continue this practice moving forward to ensure that NERC standards and requirements do not duplicate the NIST Framework.

Likes 0

Dislikes 0

Response

Joseph Amato - Joseph Amato On Behalf of: Darnez Gresham, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Joseph Amato

Answer

Document Name

Comment

We compliment the standard drafting team on great progress at addressing industry comments submitted during the last posting. While we are providing few comments on the standards themselves, we believe some changes are needed to several definitions. Since there is no ballot for the definitions alone, we will be voting negative on CIP-005, the standard that we think is most affected by issues with the definitions.

We request that NERC propose consolidation of the effective dates for CIP-004-7 and CIP-011-3 with the effective dates of this project. This would reduce the administrative burden of having to implement multiple versions for these two standards within a short time period.

Likes 0

Dislikes 0

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer

Document Name

Comment

CHPD found in its review of Draft 3 drafting errors such as comma splices and other errors which lead to significant changes to the intended meaning. CHPD respectfully encourages the SDT to take the amount of time needed to ensure Standards read as indended.

With regards to the definition of PCA and CIP-007 R1.3, CHPD firmly believes there still has been no demonstrated risk of hardware-based virtualization attacks that warrant this requirement. CISA's Known Exploited Vulnerabilities Catalog | CISA only lists a single VM escape vulnerability, which was patched before it was disclosed, and is disputed by the vendor as being in the wild. While a number of VM escape techniques have been disclosed, all have been patched and saw no confirmed exploitation in the wild.

Even speculative execution vulnerabilities like Spectre and Meltdown have not seen any confirmed exploitation in the wild and are effectively patched. Future vulnerabilities can be effectively managed by a Responsible Entity's CIP-007 R2 patching program (or mitigated by a mitigation plan if patching is not possible) and CIP-010 R3 Vulnerability Assessment program. This requirement only serves to restrict entities on architectures and to increase the cost of virtualization making it untenable.

We can also look to NIST 800-125A, Security Recommendations for Server-based Hypervisor Platforms. While VM Process Isolation is considered the first and possibly most important of the baseline functions, preventing VMs from sharing CPU or memory is not listed as any of the security recommendations to secure hypervisor baseline functions.

Looking to the technical aspects, it is CHPD’s opinion that this requirement misues the functionality of DRS (or similar for non-VMware vendors) in ways that were not intended. DRS affinity rules were not intended as a cyber security tool to prevent side channel attacks, but are intended to ensure availability and performance of VMs, as DRS is fundamentally a tool to allocate distributed resources. There are typically three types of rules; VM-to-VM affinity rules which ensure VM stay together for performance reasons, VM-to-VM anti-affinity rules which ensure that VMs stay apart for redundancy reasons incase a host fails, and VM-to-host rules, which ensure that VMs either stay connected to a specific physical resource. Because DRS rulesets were not intended for security, affinity rules do not generally allow you to specify groups of VMs and cannot share CPU with another group of VMs. That means, for example, an EACMS VM would need to have a rule for every VM that it cannot share CPU and memory with to comply with this requirement. Even if a Responsible Entity were to do this, this would create a massive web of affinity rules that would be unmanageable and potentially create a reliability issue in the event of a hardware failure, where critical VMs might not be able to find a suitable host to run on given affinity restrictions.

Setting aside the security and technical problems, the requirement itself is not clear in what it allows. It is very easy to interpret the requirement as contradicting the definition of SCI. There is a very fine line drawn with the terminology in the definition of SCI ("cluster") and the wording of CIP-007 R1.3 (sharing of CPU and memory). Some might interpret the specific hosts allowed to host CIP devices (according to the affinity ruleset) as the "cluster", meaning that R1.3 essentially contradicts the definition of SCI. There is also the question of if a high watermarked BCA still counts as its Medium Impact self. Even though you must treat it as a high impact PCA, it is still fundamentally a medium impact BCA and according to the requirement, it cannot coexist on the same CPU and memory as it is of a different impact classification. The language of R1.3 combined with the definition of SCI creates too vague of a security control to implement without significant compliance risk.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE recommends including an acronyms section at the beginning of each standard so the terms are clear and consistent.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	
Document Name	

Comment

We compliment the standard drafting team on great progress at addressing industry comments submitted during the last posting. While we are providing few comments on the standards themselves, we believe some changes are needed to several definitions. Since there is no ballot for the definitions alone, we will be voting negative on CIP-005, the standard that we think is most affected by issues with the definitions.

We request that NERC propose consolidation of the effective dates for CIP-004-7 and CIP-011-3 with the effective dates of this project. This would reduce the administrative burden of having to implement multiple versions for these two standards within a short time period.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	
Document Name	

Comment

The SCI acronym has not been defined as "Shared Cyber Infrastructure" in the proposed CIP-002, CIP-005, CIP-007, CIP-009, or CIP-010 Standard revision. The drafting team may consider defining all acronyms or not defining any acronyms as conforming changes to promote consistency within the CIP Standards.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1,3,5,6, Group Name Santee Cooper

Answer	
Document Name	

Comment

When will the Guidelines and Technical Basis that was removed from the Standards be available in the Technical Rationale or Implementation Guidance?

Likes 0	

Dislikes 0

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer

Document Name

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).

Likes 0

Dislikes 0

Response

George Brown - Acciona Energy North America - 5

Answer

Document Name

Comment

Acciona Energy supports Midwest Reliability Organization’s (MRO) NERC Standards Review Forum’s (NSRF) comments on this question.

Likes 0

Dislikes 0

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer

Document Name

Comment

TFE

SRP has recognized that for the standards and requirements where technical feasibility exemptions currently exist, the language has been removed and now uses the verbiage “per system capability”, this leads us to believe that requirements where TFE’s were available will no longer have the ability to file a TFE. SRP recommends a definition be created explaining what “per system capability” is for BES cyber systems and associated cyber assets.

CIP-002-7

Would like confirmation how or if the Guidelines and Technical Basis for CIP-002 which includes the BROS will be changed. The section now states "This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from the CIP-002- 5.1a standard to preserve any historical references. No modifications have been made."

CIP-007-7

Need some clarification on CIP-007-7 R1.1. The previous rationale states that ports and services should be managed on the cyber asset level and not just on the firewall. The new rational and wording seems a bit vague and can easily be interpreted that blocking ports and services can be done on a system level (i.e. the firewall of an ESP)

CIP-010-5

R1.1 – Would like a little more clarity on the requirements for this. The new language seems a bit vague. An example scenario:

We add a new asset which previously would have required it’s own baseline configuration but does not change any of the existing controls for CIP-005 and CIP-007. Do we not need to document the change? How would we know existing states of our assets to know what we are doing constitutes a change? Would impacted security controls be on particular systems or for all of our assets? An example of this would be changing a port that is used in a particular ESP. Would future additions of devices using this same port on different ESP’s constitute a change?

Would we be required to document changes within a timeline (30 days) like in the current R1.3?

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	
Document Name	

Comment

The proposed revision improves and makes much clearer the obligations on entities when using virtualization technologies.

Suggest modify SCI infrastructure model such that compute SCI may host mixed trust VCAs consistent with the model applied for shared storage and networking resources, similar to NIST guidance. This change would support innovation and support adoption of emerging technologies.

Likes 0	
Dislikes 0	

Response

Joni Jones - Wabash Valley Power Association - 1

Answer	
Document Name	

Comment

no further team comments. Thank you

Likes 0	
Dislikes 0	

Response
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC Entity Monitoring

Answer	
Document Name	

Comment
None.

Likes 0	
Dislikes 0	

Response

Response to Comments

Project 2016-02 Modifications to CIP Standards Virtualization | Draft 3 Posting ending April 12, 2022

Background Information

Project 2016-02 (1) addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and (2) considers the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for Standard Drafting Team Consideration (V5TAG Transfer Document).

The V5TAG, which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP Version 5 standards and to support industry's implementation activities. During the V5TAG's activities, it identified certain issues with the CIP Reliability Standards that would be better addressed by a standard drafting team (SDT) for the CIP Reliability Standards. The V5TAG developed the CIP Version 5 Transition Advisory Group Issues for Consideration document to formally recommend that the SDT address these issues and consider modifications to the standard language during the standards development process. Among other issues, the V5TAG stated "The CIP Version 5 standards comments.

Draft 3 of the Virtualization standards were posted for comment February 18 – April 12, 2022. There were 85 sets of responses, including comments from approximately 187 different people from approximately 125 companies representing 10 of the Industry.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact Vice President of Engineering and Standards Howard Gugel (via email) or at (404) 446-9693.

The standard drafting team (SDT) considered all comments received and developed the following list of themes per question and has responded to those themes below. If you have questions, contact Senior Standards Developer, Jordan Mallory (via email) or at 404-446-2589.

Question 1

The SDT has redefined Shared Cyber Infrastructure (SCI) such that it now focuses on cyber infrastructure that shares its hardware resources among Virtual Cyber Assets (VCAs) of different impact levels only, which then subjects the SCI to additional requirements. Virtualization infrastructure that only hosts VCAs or associated VCAs of the same impact level is no longer SCI and requires no re-categorization from current state. The SDT also removed the SCI identification changes from CIP-002. The SDT believes this greatly simplifies SCI. Do you agree with the proposed change?

Q1 Comment Themes:

- Request for Implementation Guidance (IG) related to SCI

- Confusion regarding how to treat clustered versus standalone
- Clarification for where VCAs can be hosted
- SCI should not be limited to only mixed trust scenarios
- Clarification for granularity of affinity controls
- Treatment of computational workload sharing systems
- Request for further clarification of SCI
- Electronic Access Control or Monitoring Systems (EACMS) with multiple impact ratings appear to require separation
- Complexity introduced by SCI increases compliance risk
- Consensus on treatment of Virtualized assets has not been established
- Confusion if re-categorization of all assets is needed
- Treatment of Cluster versus LPARs partitions
- SCI that hosts only ancillary systems like EACMS, Physical Access Control Systems (PACS) have a different risk than ones that host BES Cyber Systems (BCS)
- High-water marking is easier than SCI, misconfigured hypervisors

  SDT Response: The SDT agrees that more scenario-based technical guidance is needed. The SDT will create more technical guidance that includes many of the scenarios suggested by the commenters.

- SCI and other forms should be included in CIP-002

  SDT Response: The SDT's SAR does not include scoping for modifying CIP-002 identification requirements to include cyber system classes that are not tied to virtualization. In draft 2, the SDT did include SCI only, but pulled that from draft 3 due to stakeholder comments. The SDT notes a new SAR has been drafted and assigned to another project that will include this issue.

- Outside of SAR
- Cyber Asset expands Scope to non-Virtual assets that was not previously included (include SAN)

  SDT Response: The SDT disagrees that the scope is expanded and that any new types of Cyber Assets are being included that were not before. The SDT is adding a new option for those Cyber Assets that support different impact ratings.

- Clarification for dormant vs non-dormant

  SDT Response: The SDT agrees and has made modifications to definitions to eliminate the use of "non-dormant", include "currently executing", and exclude "dormant images" phrasing.

- Write a separate standard for virtualization

SDT Response: The SDT is adding approximately three requirement parts to individual requirements in the CIP standards to apply to situations where multiple impact rated virtual systems may share common hardware. The SDT does not agree that a separate CIP standard is required. With the new SCI definition, the vast majority of the existing CIP requirements apply to SCI as well, therefore a SCI focused standard would require a mass duplication of existing requirements.

- Fiber channel switches or NAS configurations? How are the transport networks to be treated?

  SDT Response: The SDT intentionally decided not to include network in the SCI definition due to the overly broad inclusion that this would create, however the network elements would need to be assessed for BES Cyber Asset (BCA) inclusion as part of the CIP-002 process. For situations where the switches are critical to the function of the BCS they support, the SDT asserts that they are intended to be included in that evaluation and included as BCS. In cases where the SCI is used for systems not identified as BCA and as such not protected by an ESP, the SDT recognizes that the transport network for either fiber channel or NAS configurations could expose the storage device identified as SCI to additional surface attacks on networks outside of an identified ESP. However, the SDT asserts that these risks are minimal as the systems being hosted there would normally consist of systems like EACMS, PACS, or similar less critical systems that have traditionally already been hosted outside of the protection of an ESP. The Management Interfaces of the shared storage device identified, as SCI would need to be protected under the revised CIP-005 Requirement R1 Part 1.3 to permit only needed routable protocol communications and would assume the requirements of the systems that it supports based on the usage of SCI in the applicable systems in CIP requirements across the standards.

- Clarification on treatment of SCI in CIP-006/008/009

  SDT Response: The SDT has added SCI explicitly into several CIP-006 requirements and requirement parts. In the previous draft, it was implicit in that physical protection of VCAs entails physical protection of the hardware on which they execute, but it is now explicit in the Applicable Systems column. For CIP-008, SCI is applicable to cover the scenario where the virtualization underlay, such as the hypervisors, are being attacked or exploited but may not have reached the VCAs. For CIP-009, SCI is intentionally not applicable as entities may not necessarily plan to restore the SCI in order to restore the needed functionality of the BCS. If the entity must restore the SCI in order to restore a BCS, then the SCI should be included in the restoration plan for the BCS. The 'forensic' data preservation Requirement R1 Part 1.5 in CIP-009 does include SCI as if a VCA is compromised, preserving the data concerning the SCI could be equally beneficial in an investigation.

- More evidence required at Lows for SCI

  SDT Response: The SDT is addressing the scenario where communications may be occurring with *only* the SCI and not communicating with the VCAs it may be hosting that are part of a low impact BCS. Such communications should be subject to Section 3 of Attachment 1, as well as any TCA/RM (Section 5) connections to the SCI on which BCS execute.

Question 2

The SDT has reinstated the currently approved ESP definition and appended language to allow for zero trust models. Do you agree with the proposed change?

Q2 Comment Themes:

- Request for IG related to ESP/EAP
- Desire to implement boundary and granular access control
- The existing ESP definition is adequate
- Confusion about the use of "Cyber Asset Interface" (existing language)
- Confusion about EAP relationship to requirement language
- ESP becomes confusing without inside/outside concept

  SDT Response: The SDT agrees that more technical guidance is needed. The SDT will create more technical guidance that includes many of the scenarios suggested by the commenters.

- ESP has redundant characteristics

  SDT Response: The SDT agrees the two parts of the definition could be considered redundant as the additional language at the end could be considered a superset of the first part. However, the SDT in response to comments in previous drafts has kept the first part of the definition as-is in order to account for isolated networks that have no EAP and to insure 100% backwards compatibility. However, the additional language allows flexibility for zero-trust type architectures where access control is not based on network topology.

- Clarification for treatment of host-based firewalls
- Reinstated ESP definition but refocused on to/from BCS
- Add one or more to EAP definition

  SDT Response: The SDT agrees that more clarification is needed. The SDT has added to the EAP definition the phrase to and from “one or more” BES Cyber Systems to clarify that an EAP can control communications to a grouping of hosts. As well, the SDT added the phrase “on an EACMS” to help clarify the host-based firewall scenario.

- Zero Trust is not included in the ESP/EAP definition
- EAPs appear to be required in the second part of the ESP definition

  SDT Response: The SDT included the option for “a logical boundary defined by one or more EAPs” in the ESP definition specifically to allow for zero trust architectures. The EAP definition was also updated to include “policy enforcement points” as an option also for zero trust implementations. This allows these two definitions to work together and not prescribe that access control be only at a ‘Cyber Asset interface’ on an ESP that is only a “border surrounding a network”. As to the requirement for an EAP in the ESP definition, the SDT asserts the second half of the definition is an “or” and is a separate option for implementing an ESP. The first half of the definition, as the currently approved language, requires no EAP and remains that way to allow for isolated networks with no external connectivity.

- EAP does not include PCA

SDT Response: The SDT agrees and has added “and their associated PCA’s” to the definition.

Question 3

The SDT modified the ERC definition from the "outside the asset containing" reference point in the previous draft back to an ESP reference point. Do you agree with the proposed change?

Q3 Comment Themes:

- Change ESP to EAP in ERC Definition

  SDT Response: The ESP is used in order to capture the grouping concept an ESP allows and to better align with the IRA definition.

- Keep existing ERC definition
- Create separate definition for ERC in Zero Trust

  SDT Response: The SDT disagrees as the ERC definition needs two updates. One to update it to allow for other forms of the remote client such as VCA, and two, to remove the "inside/outside" concept which does not align well with zero trust concepts. The SDT asserts that "from a Cyber Asset outside of its associated ESP" and "through an ESP" are essentially the same and a separate definition specifically for zero trust architectures is not necessary.

- Create definition for Zero Trust

  SDT Response: The SDT does not use the term Zero Trust within any requirements or definitions and as such asserts a definition is not necessary. Zero Trust concepts are outlined in detail elsewhere (e.g., NIST 800-207) and the SDT has taken the tact of simply removing any prescriptive language that would preclude the implementation of these concepts and replacing it with more objective language. The SDT believes this is a superior approach to defining the term and then writing prescriptive language concerning its implementation.

- Traffic between ESPs would be included in the ERC definition

  SDT Response: The SDT agrees that ERC would include external routable protocol traffic that is destined for another ESP. However, such traffic is excluded from the IRA definition. The SDT is more clearly delineating between ERC and IRA terms so they are not dependent on one another.

Question 4

The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change?

Q4 Comment Themes:

- IRA does not originate from an Intermediate system, add "that is not an intermediate system"

  SDT Response: The SDT agrees and has added the exclusion within the IRA definition for Intermediate Systems to avoid a recursive requirement for Intermediate Systems ("hall of mirrors").

- Consistency between lead-in on 2.1 and 2.2 (For all IRA, vs permit authorized)

SDT Response: Please see the answer to this comment under the same theme in Q7.

- IRA must initiate from external to ESP; Concerns about management systems treated as EACMS outside the ESP.

  SDT Response: The SDT asserts that the IRA definition is broad as it is defined in terms of a 'Cyber System' target inside an ESP. However, the definition is not the requirement scope and the requirement (CIP-005 R2.1) scopes IRA to only high and medium impact BCS, their associated PCAs, and any SCI that is supporting them. This is in keeping with the philosophy that glossary definitions merely define what something is, not scope of requirements nor requirements themselves. Should scoping change in the future, it can occur in the standard and its requirements, not in the glossary.

- System-to-system missing from IRA
- Clarification for user initiated (Scheduled task vs human on keys)

  SDT Response: The SDT agrees and has added the exclusion for system to system process communications that is in the current definition back into the proposed IRA definition.

- IRA required for all SCI?

  SDT Response: The SDT asserts that IRA is not required for all SCI. CIP-005 Requirement R2 Part 2.1 only applies to SCI "supporting an Applicable System in this part" and that requirement part only includes high and medium impact BCS and their associated PCAs. SCI that only supports an EACMS (that is not dual-classified as a PCA due to its location) would be an example of SCI that is not included.

- Call for CIP-015
- Too much change

  SDT Response: The SDT disagrees that such a major restructuring of the body of CIP standards is needed. The SDT is making modification to include a single scenario of the Responsible Entity converting from routable to non-routable before reaching an in-scope system. The SDT asserts this addition does not call for a major restructure or its own standard for this single scenario.

- IRA too broad; includes serial, may not be able to control outcome

  SDT Response: The SDT agrees that where the routable to non-routable conversion occurs matters. The SDT has made modifications to that bullet within the IRA definition to specify that it is in scope only when the Responsible Entity does the protocol conversion. The SDT asserts this clarifies the situation where at a substation or generator an entity may have a serial or non-routable protocol from their WAN connection they interface with, however in another entity's Control Center upstream the data is eventually converted to a routable protocol. This clarification in this bullet requires the Responsible Entity, if they perform the protocol conversion and allow IRA over it, they must implement CIP-005 R2 requirements on the routable protocol portion of the path.

- Request for IG

SDT Response: The SDT agrees that more technical guidance is needed. The SDT will create more technical guidance that includes many of the scenarios suggested by the commenters.

- Add "of a BCS" to the end of the 3rd bullet in IRA

  SDT Response: The SDT disagrees, as this would unnecessarily limit the scope of SCI that is capable of being remotely accessed with IRA. For example, SCI that is hosting only a PACS or EACMS would be excluded.

- Include definitions in the standard

  SDT Response: Approved definitions are confined to the NERC Glossary of Terms and there is no place within the standard template for definitions to be repeated within the standard.

Question 5

The SDT modified the VCA definition primarily to include the ability to host them on numerous asset types other than SCI. This allows for current state, where entities consider hypervisors as BCA, EACMS, etc. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Q5 Comment Themes:

- Clarify excluding logical instance that are being actively remediated
- Define Active Remediation

  SDT Response: The SDT has modified the PCA and VCA definitions to clarify that the scenario intended in these exclusions is a VCA that is being actively remediated "in an environment that isolates routable connectivity from BES Cyber Systems." The SDT asserts that "Remediation VLAN" is too technically prescriptive and using VLANs may be a very common but not the only way this functionality is implemented.

- Clarify non-dormant (possibly dormant as an exclusion)

  SDT Response: The SDT agrees and has made modifications to definitions to eliminate the use of "non-dormant", include "currently executing" and exclude dormant images

- Clarify where a VCA can exist
- Clarify non-SCI cluster treatment
- Clarify hosting on other types than SCI

  SDT Response: The SDT agrees that more scenario-based technical guidance is needed. The SDT will create more technical guidance that includes many of the scenarios suggested by the commenters.

- Add containers to VCA

SDT Response: The SDT disagrees as we have considered this path and there are numerous issues with the remainder of the CIP standards should this occur. Considering packaged applications differently than other installed software on a CA or VCA, namely by considering an application equal with a CA or VCA causes a large degree of complexity and technical feasibility issues.

- IRA cannot be from a VCA because VCA is limited to a CIP type

  SDT Response: The SDT agrees and has removed "from a Cyber System" from the definition. The form the remote client takes (CA, VCA, SCI) is not material to the definition and has been removed. Thanks for the comment!

- VCA Definition: Replace "On a virtual machine" with "of a virtual machine"

  SDT Response: The SDT has made other changes to the VCA definition in response to other comments that now make "on a virtual machine" the correct form of this phrase as now it refers to a logical instance "currently executing on a virtual machine".

- TCA Clarification missing from VCA

  SDT Response: The SDT will produce more technical guidance that describes two forms of virtual TCAs and the rationale for why one form of TCA is not a required hosting platform.

Question 6

The SDT modified numerous other glossary terms. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Q6 Comment Themes:

- Concerns about describing EAPs

  SDT Response: The SDT agrees as in zero trust methodologies there may be many EAPs involved. The SDT has added "on an EACMS" to the definition of EAP to help clarify this issue.

- Clarification for PCA definition sharing CPU and memory with hypervisor
- Clarify excluding logical instance that are being actively remediated

  SDT Response: The SDT has modified the PCA and VCA definitions to clarify that the scenario intended in these exclusions is a VCA that is being actively remediated "in an environment that isolates routable connectivity from BES Cyber Systems." The SDT asserts that "Remediation VLAN" is too technically prescriptive and using VLANs may be a very common but not the only way this functionality is implemented.

- Treat VM TCA on a TCA the same as VM TCA on other types

  SDT Response: The SDT will produce more technical guidance that describes two forms of virtual TCAs and the rationale for why one form of TCA is not a required hosting platform.

- Additional criteria in PCA adds complexity

SDT Response: The SDT agrees that the additional criteria adds complexity. However, the term PCA exists to define other cyber systems that "share" something with a BES Cyber System in such a way that they must be protected in a commensurate way, as they can be pivot points for an attack against the BCS. This 'sharing' has traditionally been only routable protocol networks; being a network peer of a BCS inside the ESP. With virtualization, another form of sharing is now available; the sharing of the execution environment – CPU and memory. Therefore, the SDT asserts the additions are necessary, however, it is not required that an entity implement in such a way that this new addition is in play.

- Definitions (such as VCA) are not clear and confusing

  SDT Response: The SDT will be producing more technical guidance for many definitions.

- Change "Acronym only " in the definition table

  SDT Response: The SDT agrees that the definition of BES Cyber System, the "Acronym only" in the proposed definition column was a note and not the definition. The SDT will fix this for the next posting.

- Management interface broader than just SCI

  SDT Response: The SDT agrees and has removed the scoping "of SCI or an EACMS" from the definition. This is in keeping with the keeping glossary terms in line with a dictionary and able to be used in other standards, while scoping and requirements are contained within requirement statements within the standards. The scoping of which Management Interfaces and what to do to them is within the CIP standards.

- ESP has been removed from the Intermediate system definition

  SDT Response: The removal of "where" an Intermediate System must be implemented has been purposefully removed from the definition and moved to an actual requirement part in CIP-005 R2. This is in line with our philosophy to put scoping and requirements in the standards and not in definitions. An entity that does not implement an Intermediate System correctly should have a requirement that is violated, not simply have no Intermediate System at all because they don't meet a requirement embedded in the definition.

- Clarification for addressing host-based firewalls

  SDT Response: See response to this theme in Question 2 above.

- Put lights out back into the Management Interface definition

  SDT Response: The SDT used this phrase in earlier drafts and received multiple comments it was too vendor-specific and to remove it with some suggestions to return to our draft 1 language. This is the path the SDT has taken in response to comments on draft 2. The SDT declines to change this back at this time.

- Add containers to VCA

  SDT Response: The SDT disagrees as we have considered this path and there are numerous issues with the remainder of the CIP standards should this occur. Considering packaged applications differently than other installed software on a CA or VCA, namely by considering an application equal with a CA or VCA causes a large degree of complexity and technical feasibility issues.

- Additional Clarification for "Cyber System"

  SDT Response: The SDT asserts that "Cyber System" is being proposed as a new definition merely as shorthand for the current 3 "forms" an in-scope object can take – CA, VCA, or SCI. This allows us to use this one term throughout the CIP standards where any form is allowed. This also allows, should more forms be needed in the future, a way to quickly add it to the standards without modifications to the entire suite.

- Put back examples of removable media, add new types

  SDT Response: The SDT declines this proposed change at this time. The SDT removed the examples as they become outdated or obsolete as technology continues to change.

- Preapprove Definitions before posting changes to standards

  SDT Response: The SDT disagrees, as many will not vote to approve terms (particularly technology terms) and definitions in a vacuum with no context as to how those definitions will be used. Also at times terms are created to match the requirements, such as IRA. Many may say that the IRA definition, in a vacuum, is too restrictive, however it is defined so that it matches scenarios where the CIP-005 R2 requirements can be met without affecting functionality or reliability of systems.

- Management Interfaces (such as vcenter) are on a separate system, may only have CIP-005 Part 1.3.

  SDT Response: The SDT asserts that some Management Interfaces for SCI are hosted on VCAs on the SCI and thus are implicitly covered in all SCI scoped requirements. However, in the scenario where the Management Interface is hosted separately on separate HW, the entity should consider in that case if that Cyber Asset is either a BCA or EACMS.

- Cyber Asset includes software, all hosted VCA are included in the definition
- When requirements are different it includes all requirements

  SDT Response: The SDT agrees and has modified the Cyber Asset definition to explicitly exclude VCAs from being software or data of the Cyber Asset. The SDT also modified the VCA definition to exclude the hardware from the VCA definition.

- Remove first bullet of Reportable Cyber Security Incident

  SDT Response: The SDT asserts the first bullet is needed for low impact systems.

- Clarifications for removing the requirement from the Intermediate System definition

SDT Response: The SDT will provide further clarification in future webinars and TR concerning the removal of requirement type language from this definition.

- Clarification for exclusions in Management Interface Definitions

  SDT Response: The SDT has agreed that the exclusions may add more confusion than clarity and has removed the exclusion. Physical interfaces such as touch panels and power switches already do not meet the 3 bullets in the definition.

- Does management Interface include Bluetooth?

  SDT Response: No, Bluetooth and other wireless technologies are transport to a Management Interface; they are not the Management Interface.

- Does not believe that VM escape is a demonstrated risk

  SDT Response: While the SDT agrees that most VM escape risks are in software and patches are typically quickly available, there are hardware-based attacks such as https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42114 for which there are no software patches. In SCI scenarios, the criticality of BES Cyber Systems we assert warrants requiring VCA's of differing impact categorizations to not share CPU or memory simultaneously due to risks such as this CVE.

- VCAs could be considered TCAs if left less than 30 days

  SDT Response: The SDT asserts that this is not an issue specific to virtualization changes and applies equally to any physical cyber asset that does not remain connected for 30 days or more. However, the SDT notes that the TCA definition as currently approved lists TCA uses such as data transfer, vulnerability assessment, maintenance, or troubleshooting. Performing BES functions that would meet the definition of BCA, or EACMS/PACS functions would mean that system meets those definitions.

- Clarification for "prior to introduction to an ESP" regarding the PCA definition

  SDT Response: The SDT has modified the PCA and VCA definitions to clarify that the scenario intended in these exclusions is a VCA that is being actively remediated "in an environment that isolates routable connectivity from BES Cyber Systems." The SDT asserts that "Remediation VLAN" is too technically prescriptive and using VLANs may be a very common but not the only way this functionality is implemented.

- PCA definition does not have "Highest rated impact" on the 2nd bullet

  SDT Response: The SDT asserts that the only systems that have an impact rating are BES Cyber Systems. PCA's are only "associated with" a BCS that has an impact rating, they do not have one themselves.

Question 7

The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Q7 Comment Themes:

- No ESP for SCI that only hosts EACMS

  SDT Response: The SDT agrees and has modified the applicability of CIP-005 R2.6 to exclude SCI that is not supporting a high or medium impact BCS or associated PCAs.

- Change to ESP to EAP in CIP-005 1.2

  SDT Response: The SDT asserts that EAP clarifies ESP and ESP is used in this requirement part to allow for the grouping of EAPs on an ESP such as in the case of distributed policy-based networking (i.e., zero trust).

- Consistency between lead-in on 2.1 and 2.2 (For all IRA, vs permit authorized)

  SDT Response: The SDT agrees and has made modifications to the Requirement Parts in CIP-005 R2 so that all parts begin consistently.

- Remove "authorized" and "if any" from IRA

  SDT Response: The SDT put “authorized” in the requirement part to clarify that should an attacker use some novel method to establish an unauthorized Interactive Remote Access capability not involving the entity’s Intermediate System, that would not constitute a violation of this requirement to implement an Intermediate System. The SDT does agree that the “if any” does not add any additional clarity to the requirement and has deleted that phrase.

- SCI and other forms should be included in CIP-002

  SDT Response: The SDT’s SAR does not include scoping for modifying CIP-002 identification requirements to include cyber system classes that are not tied to virtualization. In draft 2, the SDT did include SCI only, but pulled that from draft 3 due to stakeholder comments. The SDT notes a new SAR has been drafted and assigned to another project that will include this issue.

- Remove “(such as encryption)” CiP-005 R1 Part 1.4

  SDT Response: The SDT agrees and has removed the example from the requirement part and has moved it to the measures.

- Significant Effort to control Management interfaces to BCA and PCA

  SDT Response: The SDT asserts the applicability of Requirement Part R1.3 is only for Management Interfaces of SCI or EACMS and not directly to the BCA’s or PCA’s.

- Recommendation to renumber CIP-005 R1.4 to 1.6 for consistency with previous version

SDT Response: The SDT agrees and has moved the new R1.4 to the end as R1.6 to avoid any unnecessary renumbering of existing requirements within entity's programs.

- Clarification for vendor remote access and connections

SDT Response: The SDT has not made any changes to vendor remote access and refers the commenters back to the Technical Rationale documents from Project 2019-02 for explanation of those terms.

- Split SuperESP requirement back into Physical CIP-006 and Logical CIP-005
- Concern with Super ESP control in 1.4; requires physical security to fulfill a logical security control

SDT Response: The SDT asserts that these requirements have the security objective of protecting data within an ESP and allow for logical or physical options depending on the circumstance. The SDT is allowing for "across the region" as well as "across the hallway" scenarios. If some form of physical protection was required with no other option, the SDT agrees that would belong in CIP-006, but as one option among several, we assert the consolidation into CIP-005 for protecting communications within an ESP that may span PSPs belongs primarily in CIP-005.

- Clarification for handling out-of-band management

SDT Response: The SDT asserts management interfaces only apply to SCI and EACMS that enforce an ESP. Other forms of management interfaces are not addressed in our SAR.

- Don't refer to other requirement parts, spell out full applicability in each requirement part

SDT Response: The SDT asserts that would make Applicable Systems column rather unwieldy and could create maintenance issues going forward as other changes are made to the standards if these links between requirement parts are not explicit.

- Clarification for Encryption types that do not include integrity controls

SDT Response: The SDT will include a fuller explanation of the security objective within the TR.

- Move scoping for IRA from definition to requirements
- Move scoping for IRA from requirements to definition

SDT Response: The SDT asserts that moving requirements (such as where an Intermediate System must be implemented) out of the definition of what an Intermediate System is provides clarity. In the event an Intermediate System is implemented incorrectly (such as within the ESP), there should be a requirement that is violated rather than it being a matter of the Intermediate System not existing at all because what was implemented doesn't meet the full definition.

- Remove per system capability from 1.3

SDT Response: The SDT asserts that "per system capability" is needed because in some already known cases, such as many ILO cards, the ability to control incoming packets is available, but not the ability to control its own outgoing packets. However, many other higher order systems can do both to/from and both should be implemented.

- Dialup in 1.5 does not apply to all applicable types

  SDT Response: The SDT agrees that the "with Dialup Connectivity" only applied to the BCS and not to the associated PCAs as worded and has changed the formatting of the requirement to address this concern. Thanks for your comment.

- Part 1.6 limiting to IP may restrict future technologies, prescriptive
- Scoping to routable communication leaves other protocols unprotected

  SDT Response: The SDT agrees that specifying 'Internet Protocol' is prescriptive to a degree and may limit this requirement in the future. However, it is believed that IPv4 and IPv6 are the foundational routable protocol used worldwide with no foreseeable replacement or need for replacement. The SDT chose this because this is the technology upon which practically all malicious/suspected comms detection tools are built. The SDT chose not to attempt to build an exhaustive list of the protocols and physical transport that would be excluded from such a requirement (RS-232, RS485, Fiber channel, 4-20mA current loops, etc.) and after much discussion, found that "Internet Protocol" was the most concise and long-lived scope for this requirement part.

- Change Per System Capability back to Where Technically Feasible

  SDT Response: The Per System Capability term has been used in numerous places in the CIP standards to make technical requirements conditional upon the system's capability to implement the requirement in order to avoid the TFE process overhead when a system is simply not capable of a particular requirement.

- Prescription in where MFA must occur

  SDT Response: The SDT is clarifying where MFA must occur, but not at what individual Cyber Asset or VCA it must occur as "Intermediate System" is a system level concept. The SDT asserts that the Intermediate System is the appropriate and required place for the MFA to occur, as it is not protected by the ESP and therefore this requirement strongly authenticates the user before their traffic is allowed through an ESP to a BCS. As the Intermediate System will have access to many BCS, it is appropriate to strongly authenticate the user and determine what systems they have access to before the Intermediate System allows them access to any.

- IS can be hosted on the same hypervisor as a BCA

  SDT Response: The SDT has added requirement language to requirement Part 2.6 to prevent Intermediate Systems from being hosted on Cyber Assets or SCI that also host BCS. This reduces the risk of having a BCS sharing CPU/memory with an Intermediate System whose purpose is to host a public interface.

- System-to-system missing from IRA

SDT Response: See our response to this theme under Q4.

- Clarify humans on keyboards vs scheduled tasks for IRA

  SDT Response: The SDT has added the exclusion for 'system to system process communications' back into the IRA definition.

- No minimum level of encryption is specified in CIP-005 R1 part 1.4

  SDT Response: The SDT has stated the requirement as an objective concerning confidentiality and integrity to avoid the standard having to maintain changing lists of acceptable encryption algorithms and key lengths, etc. This is a practice also used in CIP-012. The standard also cannot reference other lists by external entities that could be updated by those entities, thus changing NERC requirements outside of the SPM and its defined processes.

- Define Remediation VLAN

  SDT Response: The SDT has modified the PCA and VCA definitions to clarify that the scenario intended in these exclusions is a VCA that is being actively remediated "in an environment that isolates routable connectivity from BES Cyber Systems." The SDT asserts that "Remediation VLAN" is too technically prescriptive and using VLANs may be a very common but not the only way this functionality is implemented.

Question 8

The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Q8 Comment Themes:

- Clarifications CPU/Memory (May be too prescriptive)
- Consider alternatives to the word "Prevent" in CIP-007 R1 Part 1.3
- Request clarifications for handling multiple impact ratings on SCI (CIP-007 R1 Part R1.3)
- No methods exist to prevent Sharing CPU/Memory on a single hypervisor

  SDT Response: The SDT asserts that in this case, the word "prevent" is the appropriate verb. In an SCI scenario, where systems of H/M/L/No impact are sharing hypervisors (e.g., within a cluster), this should only be allowed if the SCI is configured to prevent the sharing of CPU/memory resources by VCAs of different impact levels. The SDT chose to use the terms "CPU and memory resources" after considering all the various physical form factors available today for hypervisors such as HCI, frames, pods, etc. and to allow for technologies that can perform hardware partitioning within an "electronic device." The SDT has added additional examples to the Measures to help clarify this, as well as removing "in a clustered configuration" from the SCI definition as that is one, but not the only possible scenario. The SDT also modified PCA with the matching language of R1.3 "CPU or memory resources". As to methods for preventing the sharing of CPU/memory on a single hypervisor, the SDT asserts that this mainly applies today with a clustered configuration, where VCAs are sharing a group of and not a single hypervisor. In single hypervisor situations, if the SCI cannot be configured to prevent the sharing of CPU or memory resources, then the "all-in" scenario should be used where all hosted VCAs are high-water marked through the PCA definition.

- SCI that hosts only ancillary systems like EACMS, PACS have a different risk than ones that host BCS

  SDT Response: The SDT agrees and asserts that the Applicable Systems column addresses SCI based on the risk of the systems it supports.

- TFE requires additional mitigations that are not present with Per System Capability

  SDT Response: Please see SDT response to this TFE theme under Q7.

- Clarity around System Hardening table name in CIP-007

  SDT Response: The SDT asserts that system hardening is a widely understood and long held term of art in the cyber security field. It refers to the process of configuring a system to reduce the available attack surface. A primary example of hardening is to mitigate system compromise through a discovered vulnerability in an unnecessary but still enabled (usually by default) service. Therefore, R1.1 hardens systems by only exposing to a network those services that are necessary for the system's function and disabling all others. The SDT asserts that R1 includes this, plus hardening through the disabling of unneeded physical port access, as well as using affinity/anti-affinity rules in SCI scenarios – all of which are 'system hardening' techniques to reduce available attack surface. R1 no longer deals with only 'ports and services', which was the previous title of the table.

- Define/clarify accessibility in R1.1

  SDT Response: The SDT clarifies that R1.1 applies to "routable protocol network accessibility on each Applicable System". Routable protocol access to a system is through services which open listening logical ports on a local network interface. R1.1 requires that any unneeded access over such be either disabled or prevented. This is typically implemented through disabling the service so it does not execute, or by using some other mechanism in the OS that prevents requests from arriving at the listening logical port a service has opened. "Accessibility" as used in R1.1 is at the logical, routable protocol network level and does not include physical access, logon to the physical console, code on TCA/RM, etc. The SDT chose this phrasing to make the requirement more objective oriented. The entity may choose in some situations to implement this at the "port number" level, or conversely at the "enabled service" level, or some combination as appropriate to the scenario. For example, in an SCI scenario where proprietary communications are happening in the underlay between hypervisors, having a list of necessary and enabled hypervisor services may be preferable than describing proprietary port numbering schemes of a vendor. In other situations, a list of listening ports on a network interface may be preferable. Rather than prescribe one or the other, the SDT chose to lift this to the objective level of controlling "routable protocol network accessibility".

- Disagrees with the need to document both port and service in the measures

  SDT Response: The SDT agrees and has changed the 'and' to an 'or' in the first bullet of the measure, matching the same concept in the third bullet. Thanks for the comment.

- SCI definition brings additional devices into scope

  SDT Response: The SDT asserts that any "programmable electronic devices" that meet the various functional definitions (BCA, EACMS, PACS, etc.) and all the software on them have always been in scope. The SDT is making clarifications with new terms that allow these components to be treated separately, but the SDT does not see how the scope of devices has changed. For example, a storage resource that is critical to BCS functionality, without which it cannot operate, is a part of that system.

- Request for IG around firewalls with VLANs

  SDT Response: The SDT will address such scenarios (e.g., 'firewall on a stick') in CIP-005 TR.

- Request clarity for treatment of PCAs

  SDT Response: The SDT will provide further clarity in the TR documentation for the definitions.

- Does not believe that VM escape is a demonstrated risk

  SDT Response: Please see answer to this theme under Q6.

- Provide Clarity for CIP-007 R1 Part 1.3 for Storage arrays

  SDT Response: The SDT agrees that clarity is needed for the prevention of sharing CPU or memory resources when the SCI in question is a storage array to avoid issues with, for example, caching within an array controller. The SDT has added "excluding storage resources" to this requirement.

Question 9

The SDT revised CIP-010 R1 to focus on defining change, authorizing change, and verifying that CIP-005 and CIP-007 related security controls are not affected by changes. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Q9 Comment Themes:

- Clarification for scope of "Change"
- Clarify version changes with regards to new software
- Clarifications for custom software in CIP-010 R1 Part 1.3

  SDT Response: The SDT has added more description into CIP-010 R1.1 to further clarify the scope of changes under the change mgmt. program. The language now states "implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007." We have also added the clarifier "Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches." Several commenters pointed out that in the previous draft, it was unclear whether a user changing their password would be included (as passwords are the object of CIP-007 R5), so the SDT has clarified it is changes to *settings* that could weaken configured cyber security controls *required* by CIP-005 and CIP-007, which would not include individual user password changes.

- Concerns about movement away from baselines

  SDT Response: The SDT considered the more policy-based and automated virtualization technologies available today and determined to change the focus of Requirement R1 towards a security objective of authorizing upcoming changes rather than mandating the maintenance of a baseline configuration. Maintaining baseline configurations remains one possible "how", but it is no longer the only prescribed "how." The phrase "baseline configuration" has been removed from CIP-010 as a result. The items found in the CIP-010-4 "baseline" are now included in the Measures column within CIP-010-5. This maintains some compatibility with current state but allows flexibility for virtualization technologies and more dynamic and automated environments. This also ensures the focus is not on documenting past changes but the authorization of current or future changes, thus making the requirement forward looking with a clearer security objective. The SDT asserts that this requirement could not remain fully backward compatible as even if the prescribed list of "trigger" items remained, as it would need to be expanded to cover additional risk items from virtualization (such as the affinity rule configuration on SCI). However, creating and maintaining baseline configurations remains a way of implementing the change management objective and remains backwards compatible from that perspective.

- CEC specific to a part or the entire requirement

  SDT Response: The SDT asserts that CEC is only included in the R1.2 requirement part concerning testing in a separate test environment. It is not included in part R1.1 as those actions can be performed after a change in an emergency. Part R1.3 on the verification of source and integrity must be done prior to the change, and the SDT asserts that should still be required in a CEC situation.

- Proposed changes are outside SAR

  SDT Response: The SDT asserts that the changes are driven by consideration of virtualization technologies and are therefore within our SAR. With concepts such as dormant VCAs, VCA's with lifetimes of hours (such as VDI instances), automated patching/AV application via remediation VLANs, and in general a more dynamic environment for the in-scope Virtual Cyber Assets, the portions of the previous requirement requiring 'backwards-looking' documentation of certain 'baseline config' attributes within 35 days of the change needed updating for the more dynamic nature of today.

- SCI definition brings additional devices into scope

  SDT Response: Please see response to this comment under Question 8.

- Implementation plan needs more than 12 months

  SDT Response: Please see response to this comment under Question 13.

Question 10

The SDT made other revisions to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Q10 Comment Themes:

- Clarification for scope of "Change" for R2

  SDT Response: The SDT agrees that the scope of change in R2 needs to match the scope in R1. The SDT has added the same language on change scope that is in R1 into R2 to accomplish this. As for more general comments on clarifying the scope of change, see the response to this comment under Q9.

- Request clarification for "prior to becoming an applicable system"

  SDT Response: The SDT used this language in CIP-010 R3.3 to accommodate remediation VLANs and the nature of VCAs that are created/built in "the production environment". As VCA's are not physical assets brought into a physical environment but are usually built in some form of isolation on the production virtualization infrastructure, the SDT looked for phrasing that could accommodate this. Since a VCA, until its instantiated and has its 'production' connectivity cannot meet the definitions of the Applicable Systems (it has no BES impact, it does not yet control access, etc.), this phrasing allows VCAs to be built and their vulnerabilities assessed before the VCA is then moved to its production connectivity and can meet the functions within the definitions of the Applicable Systems. This is the cleanest way the SDT could solve the "chicken or egg" issue of VCAs built "in the production environment."

- Consider removing new 2nd bullet from Attachment 1, Sections 1.3 and 1.4

  SDT Response: The SDT changed the "live operating system from read only media" bullets in 1.3 and 1.4 in order to accommodate broader solutions, such as "VM Player" or VM snapshots that are discarded, etc. These other types of solutions return the TCA to a known "golden image" state prior to each use and is the same objective as "live OS from read only media" without being prescriptive as to a single technical solution. As these items are in a list of options, the SDT sees no harm in including them as an option.

- Clarification for like replacements in CIP-010 in R3.3

  SDT Response: The SDT's intent is the meaning of "like replacements" is within the remainder of that bullet point, namely "of the same type of Cyber System with a configuration of the previous or other existing Cyber System." It is the same intent and objective the requirement has had in that new systems, of a type or configuration not already assessed, should be assessed before introduction into the environment.

- Request clarification for the use of Cyber System vs Applicable System

  SDT Response: The SDT asserts that in the currently approved requirement part 3.3, the standard uses the term "Cyber Asset". The SDT changed this to "Cyber System" so that if an entity was replacing a physical Cyber Asset with a VCA of the same configuration, it would not require a new vulnerability assessment simply for the change in form. Cyber System is the term the SDT has proposed for use in situations like this where the form (CA, VCA, SCI) can vary.

- Treat VM TCA on a TCA the same as VM TCA on other types

  SDT Response: The SDT disagrees that VCA's on physical TCAs should be treated as their own distinct TCA. The SDT is addressing two different transient connection scenarios. The first scenario is a physical TCA such as a laptop. These TCA's may require older, 32-bit software and OS to connect to and configure older equipment in the field. These are often executed within VM 'player' environments on the physical TCA. The SDT asserts these packaged environments in an image file on a physical TCA should not be considered their own distinct virtual TCA. The SDT asserts that a user that is authorized to use the physical TCA should not be required to be separately authorized to execute the software they need to use on the TCA, simply because it's in an image file and executed in a VM "player" type environment on the TCA. The SDT also asserts that if the user goes to 'check out' a physical laptop to perform a job, it should not be a violation of a standard if they do not also 'check out' any VM images residing on that physical TCA's disk. That physical TCA is a 'unit' in order to perform a job and the SDT's intent is it should be treated as such. The SDT considered removing VCA's as an option for the form a TCA could take but has left it in to cover the second scenario.

  The second scenario is a more recent phenomenon where a service vendor (e.g., a pen-tester or security firm) may send an entity a VCA image (e.g., a vulnerability scanner instance) to temporarily instantiate within their virtualization environment. This VCA may only exist for a few hours and is functionally no different than the vendor bringing a physical laptop and connecting it to a physical network switch to perform the same task as a TCA. This transient VCA is not a part of the entity's CIP program and is treated as a TCA. The SDT did however add a specific exclusion for TCAs from the PCA definition so that the two definitions remain mutually exclusive. The TCA definition excluded PCA's; this makes the two mutually exclusive.

- Revert changes to keep Baselines

  SDT Response: Please see the SDT response to the baselines question under Q9.

- Clarify "version" in regard to New Software on CIP-010 R1.3

  SDT Response: The SDT agrees and has reworded the requirement to clarify that it is just not a software 'version' number change, but the installation of OS, firmware, software, or software patches. The term 'software version' is no longer in the requirement.

- Add Per System Capability for R2

  SDT Response: The SDT agrees and has added 'per system capability' to R2.

- Make Cyber System singular in R3.3;

  SDT Response: The SDT agrees and has removed the 's' so that it refers to "Cyber System".

- Changes do not appear related to virtualization

SDT Response: Please see response to comment concerning our SAR scope under Question 9.

- Request that we define Remediation VLANs

  SDT Response: See response to this issue under Q5.

- CIP-0010 R4 not scoped to associated SCI

  SDT Response: The SDT agrees and has added the word 'associated' in front of SCI in R4.

Question 11

The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

Q11 Comment Themes:

- Request clarification for CIP-003/CIP-006/CIP-009 not including SCI
- Clarification for physical protection of SCI

  SDT Response: The SDT agrees for CIP-006 that the physical protection of the SCI was implied in requiring the physical protection of the Applicable Systems. If they were VCAs, the only way to physically protect them was to protect the hardware on which they execute. However, because the VCA definition excludes the hardware, the SDT agrees it is not as clear as it could be. The SDT has added SCI to the Applicable Systems column in CIP-006 R1 and R2. For CIP-009, see response below.

- CIP-009 R1; no recovery plan required; but requires forensics for SCI

  SDT Response: The SDT, based on comments to previous drafts, removed SCI as an explicit object of a recovery plan. This is because the intent and goal of recovery is to recover the BES Cyber System functionality, which may or may not be recovered on SCI. The goal is not to recover SCI as merely SCI. Therefore, if recovering the SCI is a necessary part of recovering the BCS, then SCI should be included in the recovery plan. One example is a domain controller as an EACMS may be virtualized as a VCA on SCI. The SCI may go down and may require an extended recovery and in the meantime the entity may install Windows Server as a domain controller on a standalone server to quickly recover the functionality. However, SCI is an explicit object of the forensics requirement. In the instance that a VCA is compromised, capturing information from the SCI on which it executes is appropriate in order to investigate the compromise.

- SCI and other forms should be included in CIP-002

  SDT Response: See the response to this comment theme under Q1.

- CIP-011 R2 Part 2.1 Why is PCA a part of Part 2.1 but not R1?

  SDT Response: The SDT asserts this is existing scope not modified by this SDT under our SAR.

- Simplification of TCA mitigation bullets. Consider clarifications for new mitigations that replace Live Operating System

  SDT Response: The SDT replaced these more prescriptive bullets concerning 'live operating systems' with a more objective-based description. This was to allow for other technologies such as "VM players" that run VCA images without saving any changes made by any potential malware.

- Requests clarifications for System Capability

  SDT Response: This is a phrase that has been used in the standards since the introduction of Version 5 and this SDT is continuing to use that existing phrase. It is used to make the requirement conditional for the majority of systems for which that requirement was designed, without requiring it on every such system in existence, which does not have the capability. It allows a requirement to hit the 90-10 rule without a burdensome process.

- Treat VM TCA on a TCA the same as VM TCA on other types

  SDT Response: See answer to this issue under Q10.

- Administrative issue in CIP-008 Part 2.3

  SDT Response: The SDT agrees. This was an issue in a redline version and has been addressed by adding SCI.

- Clarify "supports any part a BES Cyber System" in CIP-003

  SDT Response: The SDT agrees after review that the "any part of" is not adding any clarity and may be confusing. The SDT has removed "any part of" phrasing.

- Vote on definitions separately

  SDT Response: See the response to the comment on "preapprove definitions" in Q6.

- "Or their successors" missing from CISA on CIP-008

  SDT Response: The SDT agrees. This was an issue in a redline version and has been addressed.

- Remove CEC CIP-006 R2.2; already covered in high level R

  SDT Response: The SDT agrees and has removed the duplicate CEC phrase in R2.2.

Question 12

The SDT has revised numerous VSL's for simplification. Do you agree with the proposed changes? If not, please provide the basis for your disagreement.

Q12 Comment Themes:

- CIP-003 Delete - "The responsible entity but failed to manage its Transient Cyber Assets"
- Per System Capability

    - CIP-004 R4.1 categories
    - CIP-005 R1.3
    - CIP-007 R4.3
- CIP-005 1.4 missing VSL

  SDT Response: The SDT has reviewed these issues and has made corrections to the VSL's. Thank you for the comments. Specific to the "per system capability" comments, those are not included in any VSLs as the system capability is determined as part of the overall determination as to whether a potential violation has occurred. Once at a stage where the VSL is needed, the system capability has already been determined.

Question 13

The SDT has revised the Implementation Plan to include the Planned and Unplanned Changes provisions and to allow for early adoption. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

Q13 Comment Themes:

- 36 month preference

  SDT Response: The implementation plan and CIP-003-X from Project 2020-03 "Supply Chain Low Impact Revisions" will be combined with this SDT's package and CIP-003-Y (after successful 2016-02 ballot) and a final CIP-003-8 and integrated single implementation plan with final timeframes will be posted for comment/ballot. At this time, the SDT is not hearing a sufficient stakeholder push for more time for the virtualization changes.

- 12 Months is not enough for Changes to planned/unplanned timeframes

  SDT Response: The SDT has made no changes to this longstanding language and is carrying it forward from previously and currently approved versions of the Implementation Plan.

Question 14

Please provide any additional comments for the SAR drafting team to consider, if desired.

Q14 Comment Themes:

- CIP-004 elimination of BSCI repositories

  SDT Response: The elimination of BCSI "repository" language was under the Project 2019-02 SDT and was successfully balloted. This SDT is carrying their successfully balloted changes forward and has made no changes to R6 other than to add SCI to the scope.

- Clarifications for Imp plan on "Upon Commissioning"

  SDT Response: The SDT has made no changes to this longstanding language and is carrying it forward from previously and currently approved versions of the Implementation Plan.

- Inconsistent use of Applicable Systems capitalization in VSL's
- Inconsistent handling of Acronyms for Definitions
- Use of BCS vs BCA inconsistent

  SDT Response: The SDT thanks you for the comments and will look for these issues as it prepares final documents for the next draft.

- SCI and other definitions are unclear about whether its dealing with on-premise virtualization or cloud

  SDT Response: The SDT is not (and it is not in our SAR) addressing cloud computing where the "programmable electronic devices" are not located on the entity's premises in one of the six CIP-002 BES asset classes listed in R1. Those six asset classes remain the scope of this version of the standards, therefore it is on-premise virtualization only.

- Implementing Affinity in SCI with multiple impact ratings is complex

  SDT Response: The SDT agrees that this is a more complex configuration option, but it has other benefits that an entity may want to take advantage of. However, the SDT notes that using SCI and affinity rules is one option and is not mandatory. The "all-in" scenario is another option without the complexity of managing affinity.

- Vote definitions separately

  SDT Response: See the response to the comment on "preapprove definitions" in Q6.

- Desire to not reuse requirement numbers (CIP-005)

  SDT Response: The SDT agrees and where possible has reordered requirement parts to better align with currently approved standards.

- No evidence of VM escape; affinity requirements not needed

  SDT Response: Please see answer to this theme in Q6.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 4 Definitions”

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the Bulk Electric System (BES). Identification and categorization of BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1. Balancing Authority

      4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

            4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-7:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of Parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** RAS that support the reliable operation of the BES; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:
"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:
The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program:
As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #			Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1			For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer of identified BCS have not been categorized or have been	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent but less than or equal to 10	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BCS, more than 10 percent but less than or equal to 15 percent of	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of identified BCS have not been categorized or have been incorrectly

R #			Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or fewer identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or fewer high or medium BCS have not been identified.	percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and BCS, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent but less than or equal to 10 percent high or medium BCS have not been identified; OR	identified BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BCS, more than 10 but less than or equal to 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 10 percent but less than or equal to 15 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or	categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of high or medium impact BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact

R #			Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than five but less than or equal to 10 high or medium BCS have not been identified.	fewer high and medium impact BCS, more than 10 but less than or equal to 15 high or medium BCS have not been identified.	BCS have not been identified.
R2			The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (Part2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of

R #			Violation Severity Levels (CIP-002-7)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than or equal to 16 calendar months of the previous approval. (Part 2.2)	less than or equal to 17 calendar months of the previous approval. (Part 2.2)	less than or equal to 18 calendar months of the previous approval. (Part 2.2)	the previous approval. (Part 2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High impact rating**
   Each BCS used by and located at any of the following:

   1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

   1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

   1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

   1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium impact rating**
   Each BCS, not included in Section 1 above, associated with any of the following:

   2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

   2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

   2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each RAS or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding

(UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in high impact rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in high impact rating, above.

2.13. Each Control Center or backup Control Center, not already included in high impact rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low impact rating

BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~third~~ fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
~~45~~53-day formal comment period with ballot	February 18 – April ~~4~~12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	~~April~~ October 2022
Board adoption	~~May~~ November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft ~~3~~ 4 Definitions"

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the Bulk Electric System (BES). Identification and categorization of BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-7:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan"

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of Parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** RAS that support the reliable operation of the ~~Bulk Electric System~~ BES; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer of identified BCS have not been categorized or have been incorrectly categorized at a lower category; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent but less than or equal to 10 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category;	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BCS, more than 10 percent but less than or equal to 15 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category;	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than 15 identified BCS have not been

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or fewer identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or fewer high or medium BCS have not been identified.	OR For Responsible Entities with a total of 100 or fewer high and medium impact and BCS, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent but less than or equal to 10 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than five but less than or equal to 10 high or medium BCS have not been identified.	OR For Responsible Entities with a total of 100 or fewer high or medium impact and BCS, more than 10 but less than or equal to 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 10 percent but less than or equal to 15 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than 10 but less than or equal to 15 high or medium BCS have not been identified.	categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of high or medium impact BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BCS have not been identified.
R2	The Responsible Entity did not complete its review and	The Responsible Entity did not complete its review and update	The Responsible Entity did not complete its review and update	The Responsible Entity did not complete its review and update for

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (Part 2.2)	for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (Part2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (Part 2.2)	for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (Part 2.2)	the identification required for Requirement R1 within 18 calendar months of the previous review. (Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (Part 2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High impact rating**
   Each BCS used by and located at any of the following:
   - **1.1.** Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.
   - **1.2.** Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.
   - **1.3.** Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.
   - **1.4** Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.
2. **Medium impact rating**
   Each BCS, not included in Section 1 above, associated with any of the following:
   - **2.1.** Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.
   - **2.2.** Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.
   - **2.3.** Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.
   - **2.4.** Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each RAS or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in high impact rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in high impact rating, above.

2.13. Each Control Center or backup Control Center, not already included in ~~H~~high impact rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low impact rating

BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. RAS that support the reliable operation of the Bulk Electric System.

For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 4 Definitions”

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7~~5.1a~~

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those ~~BES Cyber Systems~~BCS could have on the reliable operation of the Bulk Electric System (BES). Identification and categorization of ~~BES Cyber Systems~~BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and

including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. **Generator Operator**

4.1.4. **Generator Owner**

~~**4.1.5.** **Interchange Coordinator or Interchange Authority**~~

~~4.1.6.~~4.1.5. **Reliability Coordinator**

~~4.1.7.~~4.1.6. **Transmission Operator**

~~4.1.8.~~4.1.7. **Transmission Owner**

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~Special Protection System or Remedial Action Scheme~~RAS where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-7~~5.1a~~:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2.~~4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan"

~~1. **24 Months Minimum** – CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

~~**6. Background:**~~

~~This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.~~

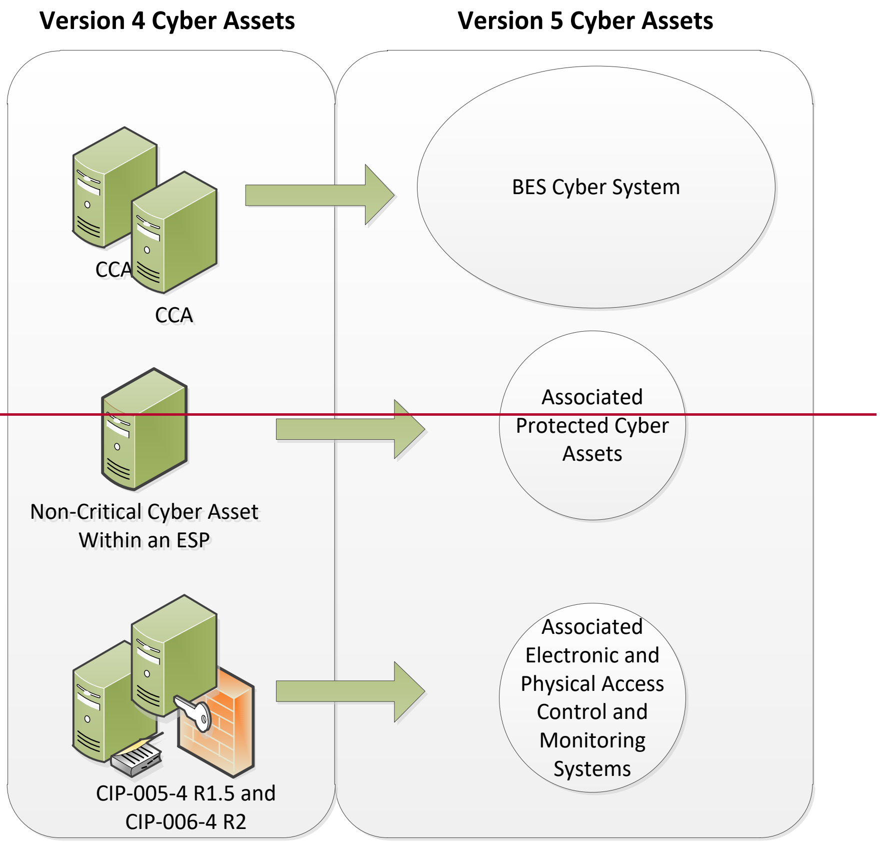
~~Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW~~

~~represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~BES Cyber Systems~~

~~One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.~~



~~In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.~~

~~Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and~~

~~compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.~~

~~It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Reliable Operation of the BES~~

~~The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.~~

~~Real-time Operations~~

~~One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.~~

~~Categorization Criteria~~

~~The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.~~

~~This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.~~

~~Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems~~

~~BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:~~

~~Electronic Access Control or Monitoring Systems ("EACMS")~~ ~~– Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.~~

~~Physical Access Control Systems ("PACS")~~ ~~– Examples include: authentication servers, card systems, and badge control systems.~~

~~Protected Cyber Assets ("PCA")~~ ~~– Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of ~~p~~Parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** ~~Special Protection Systems~~RAS that support the reliable operation of the ~~Bulk Electric System~~BES; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact ~~BES Cyber Systems~~BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact ~~BES Cyber Systems~~BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact ~~BES Cyber System~~BCS according to Attachment 1, Section 3, if any (a discrete list of low impact ~~BES Cyber Systems~~BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1~~, and Parts 1.1 and 1.2~~.

R2. ~~The~~ Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions. ~~The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.~~

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Assessment~~ Enforcement ~~Processes~~Program:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~

- ~~Complaint~~

~~1.4. Additional Compliance Information~~

- ~~None~~**~~Table of Compliance Elements~~**

Violation Severity Levels

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	~~Operations Planning~~	~~High~~	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber~~

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Systems~~BCS, five percent or fewer of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, five or fewer identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium	For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than five percent but less than or equal to 10 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact and ~~BES Cyber Systems~~BCS, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly	For Responsible Entities with more than a total of 100 high or medium impact ~~BES Cyber Systems~~BCS, more than 10 percent but less than or equal to 15 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and ~~BES Cyber Assets~~BCS, more than 10 but less than or equal to 15 identified ~~BES Cyber Assets~~BCS have not been categorized or have been incorrectly	~~Systems~~BCS, more than 15 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than 15 identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			impact ~~BES Cyber Systems~~BCS, five percent or fewer high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, five or fewer high or medium ~~BES Cyber Systems~~BCS have not been identified.	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than five percent but less than or equal to 10 percent high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than five but less than or equal to 10 high or medium ~~BES Cyber Systems~~BCS	categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 10 percent but less than or equal to 15 percent high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than 10 but less than or equal to 15 high or medium ~~BES Cyber Systems~~BCS	impact ~~BES Cyber Systems~~BCS, more than 15 percent of high or medium impact ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact ~~BES Cyber Systems~~BCS have not been identified.

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				have not been identified.	have not been identified.	
R2	~~Operations Planning~~	~~Lower~~	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (~~R~~Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (~~R~~Part2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (~~R~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (~~R~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (~~R~~Part 2.2)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-002-7~~5.1a~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the previous approval. (~~R~~Part 2.2)	of the previous approval. (~~R~~Part 2.2)	of the previous approval. (~~R~~Part 2.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

~~CIP-002-5.1a - Attachment 1~~

~~Impact Rating Criteria~~

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High i~~I~~mpact r~~R~~ating~~ (H)~~

Each ~~BES Cyber System~~BCS used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium i~~I~~mpact r~~R~~ating~~ (M)~~

Each ~~BES Cyber System~~BCS, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~ each discrete shared ~~BES Cyber Systems~~ BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each ~~Special Protection System (SPS), Remedial Action Scheme (~~RAS~~),~~ or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in h~~H~~igh i~~I~~mpact r~~R~~ating ~~(H)~~ above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in h~~H~~igh i~~I~~mpact r~~R~~ating ~~(H)~~, above.

2.13. Each Control Center or backup Control Center, not already included in ~~H~~high i~~I~~mpact r~~R~~ating ~~(H)~~ above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low i~~I~~mpact r~~R~~ating ~~(L)~~

~~BES Cyber Systems~~BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. ~~Special Protection Systems~~RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.~~

~~For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.~~

~~CIP-002-5.1a~~

~~CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."~~

~~The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber~~

~~Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:~~

~~Dynamic Response to BES conditions~~
~~Balancing Load and Generation~~
~~Controlling Frequency (Real Power)~~
~~Controlling Voltage (Reactive Power)~~
~~Managing Constraints~~
~~Monitoring & Control~~
~~Restoration of BES~~
~~Situational Awareness~~
~~Inter-Entity Real-Time Coordination and Communication~~

~~Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.~~

~~**Entity Registration**~~	~~**RC**~~	~~**BA**~~	~~**TOP**~~	~~**TO**~~	~~**DP**~~	~~**GOP**~~	~~**GO**~~
~~Dynamic Response~~		~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Balancing Load & Generation~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Controlling Frequency~~		~~X~~				~~X~~	~~X~~
~~Controlling Voltage~~			~~X~~	~~X~~	~~X~~		~~X~~
~~Managing Constraints~~	~~X~~		~~X~~			~~X~~	
~~Monitoring and Control~~			~~X~~			~~X~~	
~~Restoration~~			~~X~~			~~X~~	
~~Situation Awareness~~	~~X~~	~~X~~	~~X~~			~~X~~	
~~Inter-Entity coordination~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~	~~X~~

~~Dynamic Response~~

~~The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:~~

- ~~Spinning reserves (contingency reserves)~~
    - ~~Providing actual reserve generation when called upon (GO,GOP)~~
    - ~~Monitoring that reserves are sufficient (BA)~~
- ~~Governor Response~~
    - ~~Control system used to actuate governor response (GO)~~
- ~~Protection Systems (transmission & generation)~~
    - ~~Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)~~
    - ~~Zone protection for breaker failure (DP, TO, TOP)~~
    - ~~Breaker protection (DP, TO, TOP)~~
    - ~~Current, frequency, speed, phase (TO,TOP, GO,GOP)~~
- ~~Special Protection Systems or Remedial Action Schemes~~
    - ~~Sensors, relays, and breakers, possibly software (DP, TO, TOP)~~
- ~~Under and Over Frequency relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Under and Over Voltage relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Power System Stabilizers (GO)~~

~~Balancing Load and Generation~~

~~The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:~~

- ~~Calculation of Area Control Error (ACE)~~
    - ~~Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)~~
    - ~~Software used to perform calculation (BA)~~
- ~~Demand Response~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP,DP)~~
- ~~Manually Initiated Load shedding~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP, DP)~~

- ~~Non-spinning reserve (contingency reserve)~~
    - ~~Know generation status, capability, ramp rate, start time (GO, BA)~~
    - ~~Start units and provide energy (GOP)~~

~~Controlling Frequency (Real Power)~~

~~The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:~~

- ~~Generation Control (such as AGC)~~
    - ~~ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)~~
    - ~~Software to calculate unit adjustments (BA)~~
    - ~~Transmit adjustments to individual units (GOP)~~
    - ~~Unit controls implementing adjustments (GOP)~~
- ~~Regulation (regulating reserves)~~
    - ~~Frequency source, schedule (BA)~~
    - ~~Governor control system (GO)~~

~~Controlling Voltage (Reactive Power)~~

~~The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:~~

- ~~Automatic Voltage Regulation (AVR)~~
    - ~~Sensors, stator control system, feedback (GO)~~
- ~~Capacitive resources~~
    - ~~Status, control (manual or auto), feedback (TOP, TO,DP)~~
- ~~Inductive resources (transformer tap changer, or inductors)~~
    - ~~Status, control (manual or auto), feedback (TOP,TO,DP)~~
- ~~Static VAR Compensators (SVC)~~
    - ~~Status, computations, control (manual or auto), feedback (TOP, TO,DP)~~

~~Managing Constraints~~

~~Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:~~

- ~~Available Transfer Capability (ATC) (TOP)~~
- ~~Interchange schedules (TOP, RC)~~
- ~~Generation re-dispatch and unit commit (GOP)~~
- ~~Identify and monitor SOL's & IROL's (TOP, RC)~~
- ~~Identify and monitor Flow gates (TOP, RC)~~

~~Monitoring and Control~~

~~Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:~~

- ~~All methods of operating breakers and switches~~
  - ~~SCADA (TOP, GOP)~~
  - ~~Substation automation (TOP)~~

~~Restoration of BES~~

~~The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:~~

- ~~Restoration including planned cranking path~~
  - ~~Through black start units (TOP, GOP)~~
  - ~~Through tie lines (TOP, GOP)~~
- ~~Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)~~
- ~~Coordination (TOP, TO, BA, RC, DP, GO, GOP)~~

~~Situational Awareness~~

~~The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:~~

- ~~Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)~~
- ~~Change management (TOP,GOP,RC,BA)~~
- ~~Current Day and Next Day planning (TOP)~~
- ~~Contingency Analysis (RC)~~
- ~~Frequency monitoring (BA, RC)~~

~~Inter-Entity Coordination~~

~~The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:~~

- ~~Scheduled interchange (BA,TOP,GOP,RC)~~
- ~~Facility operational data and status (TO, TOP, GO, GOP, RC, BA)~~
- ~~Operational directives (TOP, RC, BA)~~

~~Applicability to Distribution Providers~~

~~It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.~~

~~Requirement R1:~~

~~Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.~~

~~Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.~~

~~Attachment 1~~

~~Overall Application~~

~~In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.~~

- ~~When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.~~
- ~~In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.~~
- ~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.~~

~~High Impact Rating (H)~~

~~This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some~~

~~of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.~~

~~The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.~~

~~Additional thresholds as specified in the criteria apply for this category.~~

~~Medium Impact Rating (M)~~

~~Generation~~

~~The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.~~

- ~~Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.~~

  ~~In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.~~

  ~~By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.~~

~~The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.~~

- ~~In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.~~

  ~~If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.~~

  ~~The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.~~

- ~~Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~, ~~R5.1.1 and R5.1.3.~~

  ~~IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.~~

- ~~Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.~~

- ~~Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.~~

- ~~Criterion 2.13 categorizes as medium impact those BA Control Centers that “control” 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Transmission~~

~~The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist.~~

- ~~Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.~~

- ~~Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.~~

~~It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.~~

- ~~Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:~~
    - ~~Excluded radial facilities that would only provide support for single generation facilities.~~
    - ~~Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.~~

~~The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.~~

~~Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:~~

- ~~230 kV –> 700 MVA~~
- ~~345 kV –> 1,300 MVA~~
- ~~500 kV –> 2,000 MVA~~
- ~~765 kV –> 3,000 MVA~~

~~In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:~~

- ~~For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate~~

~~connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.~~

- ~~Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~
- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

~~Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.~~

1. ~~The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.~~
2. ~~The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.~~

~~The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.~~

- ~~Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.~~

- ~~Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.~~

- ~~Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.~~

- ~~Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.~~

- ~~Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.~~

  ~~This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.~~

~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.~~

- ~~Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.~~
- ~~Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Low Impact Rating (L)~~

~~BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.~~

~~Restoration Facilities~~

- ~~Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.~~

  ~~In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.~~

  ~~The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.~~

~~Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.~~

~~BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~

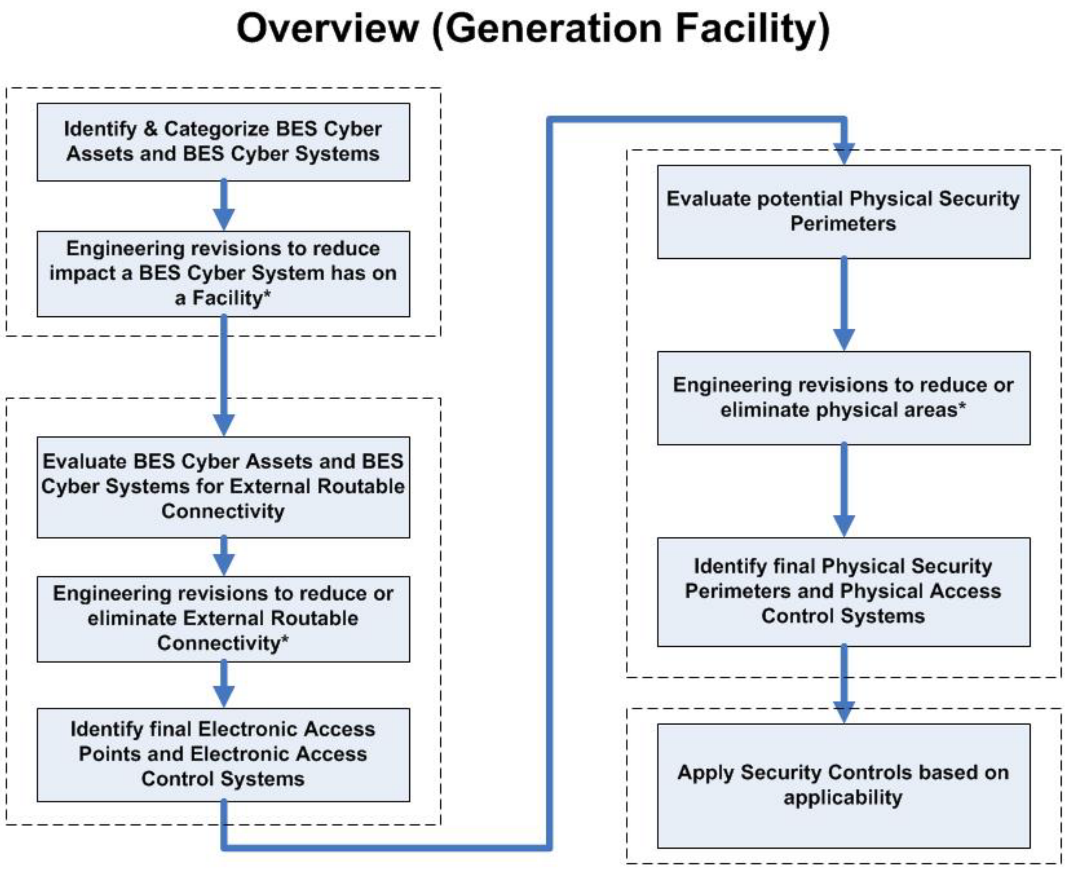
~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.~~

~~Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.~~

~~Use Case: CIP Process Flow~~

~~The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.~~



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for R1:~~

~~BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of “bright-line” criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~Rationale for R2:~~

~~The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager’s approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.~~

~~Appendix 1~~

~~Requirement Number and Text of Requirement~~

~~CIP-002-5.1, Requirement R1~~

~~R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:~~

~~Control Centers and backup Control Centers;~~

~~Transmission stations and substations;~~

~~Generation resources;~~

~~Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;~~

~~Special Protection Systems that support the reliable operation of the Bulk Electric System; and~~

~~For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.~~

~~Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;~~

~~Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and~~

~~Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).~~

~~Attachment 1, Criterion 2.1~~

~~Medium Impact Rating (M)~~

~~Each BES Cyber System, not included in Section 1 above, associated with any of the following:~~

~~Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~

~~Questions~~

~~Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."~~

~~The Interpretation Drafting Team identified the following questions in the RFI:~~

~~Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~

~~Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~

~~If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~Responses~~

~~Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~

~~The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)~~

~~Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:~~

~~The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~

~~The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.~~

~~The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:~~

~~Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1~~

~~and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1:~~ ~~**Impact Rating of Generation Resource Shared BES Cyber Systems**~~ ~~for further information and examples.~~

~~**Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?**~~

~~The phrase applies to each discrete BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 4 Definitions”

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-Y

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-Y:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links, between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. **Compliance Monitoring Process**

   1.1. **Compliance Enforcement Authority:** "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

   1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-Y)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-003-Y)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1)
OR
The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the six topics required by Requirement R1. (Part 1.2)
OR
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar</td><td>complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1)
OR
The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the six topics required by R1. (Part 1.2)
OR
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2)
OR</td><td>complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1)
OR
The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the six topics required by Requirement R1. (Part 1.2)
OR
The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2)
OR</td><td>impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1)
OR
The Responsible Entity did not address four or more of the six topics required by Requirement R1. (Part 1.2)
OR
The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by R1. (R1.2)
OR
The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager</td></tr>
</table>

R #	Violation Severity Levels (CIP-003-Y)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	within 18 calendar months of the previous approval. (R1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-003-Y)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2)
OR
The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2)
OR
The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)
OR
The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)</td><td>controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2)
OR
The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)
OR
The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (R2)
OR
The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2)
OR
The Responsible Entity failed to document the determination of whether an</td><td>according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2)
OR
The Responsible Entity documented failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2)
OR
The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)
OR
The Responsible Entity failed to implement mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)</td><td></td></tr>
</table>

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-003-Y)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>OR
The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)</td><td>identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2)
OR
The Responsible Entity failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2)
OR
The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment</td><td>OR
The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2)
OR
The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)</td><td></td></tr>
</table>

R #	Violation Severity Levels (CIP-003-Y)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR

R #	Violation Severity Levels (CIP-003-Y)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TTCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

  - Review of antivirus update level;
  - Review of antivirus update process used by the party;
  - Review of application whitelisting used by the party;

- Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process

documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. <u>TCA and Removable Media Malicious Code Risk Mitigation</u>:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, controls to maintain the known good state of the OS and software, application whitelisting practices, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of controls to maintain the known good state of the OS and software, or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the

party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~third~~ fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
~~45~~53-day formal comment period with ballot	February 18 – April 4, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	~~April~~ October 2022
Board adoption	~~May~~ November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft ~~3~~4 Definitions"

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-Y

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. **Balancing Authority**

4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. **Generator Operator**

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-Y:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links, between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports ~~any part of~~ a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1			The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the six topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or	more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the six topics required by R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or	Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the six topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in	the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the six topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of	more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to	less than or equal to 18 calendar months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the previous approval. (Part 1.2)	17 calendar months of the previous approval. (Part 1.2)		
R2			The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2,	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2,	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2,	The Responsible Entity failed to document and implement one or more cyber security plan(s) for its assets containing low impact BCS according to Requirement R2, Attachment 1. (Requirement R2)

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 4. (R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity but failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	Attachment 1, Section 3. (R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity that provides access to low impact BCS(s), per Cyber Asset capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR	Attachment 1, Section 4. (R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party	

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2)	other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3			The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR

R #			Violation Severity Levels (CIP-003-Y)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change in less than 40 calendar days of the change. (Requirement R3)	change in less than 50 calendar days of the change. (Requirement R3)	calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)
R4			The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports ~~any part of~~ a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports ~~any part of~~ a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports ~~any part of~~ a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports ~~any part of~~ a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TTCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports ~~any part of~~ a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports ~~any part of~~ a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications between Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process

documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, controls to maintain the known good state of the OS and software, application whitelisting practices, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of controls to maintain the known good state of the OS and software, or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the

party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 4 Definitions”

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-Y~~8~~

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-Y~~8~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links, between discrete Electronic Security Perimeters (ESP~~s~~).

~~4.2.3.2.~~**4.2.3.3.** Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

~~See Implementation Plan for CIP-003-8.~~

~~6. **Background:**~~

~~Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.~~

~~The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.~~

~~The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.~~

~~Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact ~~BES Cyber Systems~~BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of ~~BES Cyber Systems~~BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for ~~BES Cyber Systems~~BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation; and

1.2.6. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS shall implement one or more documented cyber security plan(s) for its low impact ~~BES Cyber Systems~~BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact ~~BES Cyber Systems~~BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

“Compliance Enforcement Authority” means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions. ~~As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.~~

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program~~Assessment Processes~~:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audits~~
- ~~Self-Certifications~~
- ~~Spot Checking~~
- ~~Compliance Investigations~~
- ~~Self-Reporting~~
- ~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None.~~

Violation Severity Levels

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	~~Operations Planning~~	~~Medium~~	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address one of the nine topics required by Requirement R1. (~~R~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address two of the nine topics required by Requirement R1. (~~R~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address three of the nine topics required by Requirement R1. (~~R~~Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 17 calendar months but did complete this review in	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address four or more of the nine topics required by Requirement R1. (Part ~~R~~1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1. (~~R~~Part 1.1)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (~~R~~Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16	within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R~~Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17	less than or equal to 18 calendar months of the previous review. (~~R~~Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by Requirement R1 by the CIP Senior

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			calendar months of the previous approval. (~~R~~Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address one of the six topics required by Requirement R1. (~~R~~Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing	calendar months of the previous approval. (~~R~~Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address two of the six topics required by R1. (~~R~~Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES	policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address three of the six topics required by Requirement R1. (~~R~~Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (~~R~~Part 1.2) OR	Manager within 18 calendar months of the previous approval. (~~R~~Part 1.1) OR The Responsible Entity ~~documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems, but~~ did not address four or more of the six topics required by Requirement R1. (~~R~~Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (~~R~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior	Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 16	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (~~R~~Part 1.2)	impact ~~BES Cyber Systems~~BCS as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (R1.2)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (~~R~~Part 1.2)	calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (~~R~~Part 1.2)		
R2	~~Operations Planning~~	~~Lower~~	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~implemented electronic access~~	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR	The Responsible Entity ~~documented the physical access controls for its assets containing low impact BES Cyber Systems, but~~ failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls for its assets~~	The Responsible Entity failed to document and implement one or more cyber security plan(s) ~~for its assets containing low impact BES Cyber Systems~~BCS according to Requirement R2, Attachment 1. (Requirement R2)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~controls but~~ failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document electronic access controls according to Requirement R2,	~~containing low impact BES Cyber Systems, but~~ failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented ~~one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2)	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to manage	Attachment 1, Section 3. (R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls but~~ failed to implement authentication for all Dial-up Connectivity ~~that provides access to low impact BES Cyber System~~BCS~~(s), per Cyber Asset~~ capability according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity ~~documented one or more incident response plan(s) within its cyber security plan(s) for~~	OR The Responsible Entity ~~documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but~~ failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for ~~Transient Cyber Assets~~TCA managed by	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets, but~~ failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	~~its assets containing low impact BES Cyber Systems, but~~ failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document the determination of whether an identified Cyber Security Incident is a	the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber~~	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for ~~Transient Cyber Assets~~TCA managed by the Responsible Entity according to	~~Assets and Removable Media, but~~ failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media ~~to a low impact BES Cyber SystemBCS~~ according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR		

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)		
R3	~~**Operations Planning**~~	~~**Medium**~~	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has~~ did not identify~~ied~~, by name, a CIP Senior Manager. OR The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				the change. (Requirement R3)		Senior Manager within 60 calendar days of the change. (Requirement R3)
R4	~~**Operations Planning**~~	~~**Lower**~~	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has used delegated authority for actions where allowed by the CIP Standards, but~~ does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 60

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels (CIP-003-Y~~8~~)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

Version	Date	Action	Change Tracking
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	

Version	Date	Action	Change Tracking
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	

Attachment 1

Required Sections for Cyber Security Plan(s) ~~for Assets Containing Low Impact BES Cyber Systems~~

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact ~~BES Cyber Systems~~BCS ratings can utilize policies, procedures, and processes for their high or medium impact ~~BES Cyber Systems~~BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. ~~b~~Between:

- a low impact ~~BES Cyber System(s)~~BCS; or
- An SCI that supports a low impact BCS ~~and a Cyber Asset(s)~~

and a Cyber System(s) outside the asset containing:

- the low impact ~~BES Cyber System~~BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact ~~BES Cyber System(s)~~BCS or SCI that a low impact BCS; and

iii. not used for time-sensitive ~~protection or control functions between intelligent electronic devices (e.g., ~~communications of Protection Systems~~using protocol IEC TR-61850-90-5 R-GOOSE)~~.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact ~~BES Cyber System(s)~~BCS or SCI that supports a low impact BCS, per ~~Cyber Asset~~system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. ~~Transient Cyber Asset~~TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact ~~BES Cyber Systems~~BCS, through the use of ~~Transient Cyber Assets~~TCA or Removable Media. The plan(s) shall include:

5.1 For T~~ransient Cyber Asset(s)~~TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA~~Transient Cyber Asset~~ capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting ~~the Transient Cyber Asset to a low impact BES Cyber System~~ (per ~~Transient Cyber Asset~~TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code~~use of live operating system and software executable only from read-only media~~;
- Review of system hardening used by the party; or
- Review of ~~O~~other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset~~TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a ~~BES Cyber System~~BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~BCS or SCI that supports a low impact BCS.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) ~~for Assets Containing Low Impact BES Cyber Systems~~

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset; and
  b. The Cyber ~~Asset(s)~~System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by ~~containing low impact BES Cyber Systems, routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset is restricted by electronic access controls to permit only inbound and outbound~~ electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. ~~is used for time-sensitive protection or control functions between intelligent electronic devices.~~ Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) ~~between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s)~~ or

lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the ~~BES Cyber System~~BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. ~~Transient Cyber Asset~~TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, controls to maintain the known good state of the OS and software, application whitelisting practices, ~~processes to restrict communication,~~ or other method(s) to mitigate the introduction of malicious code. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from

the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, ~~use of live operating systems~~use of controls to maintain the known good state of the OS and software, or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

~~3.~~ Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.~~**Guidelines and Technical Basis**~~

~~**4. Section 4 – Scope of Applicability of the CIP Cyber Security Standards**~~

~~5. Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~6. Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~7. Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES~~

~~Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~8. Requirement R1:~~

~~9. In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.~~

~~10. If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.~~

~~11. Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.~~

~~12. Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.~~

~~13. For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:~~

~~14. 1.1.1 Personnel and training (CIP-004)~~

~~15. Organization position on acceptable background investigations~~

~~16. Identification of possible disciplinary action for violating this policy~~

~~17. Account management~~

~~18. Electronic Security Perimeters (CIP-005) including Interactive Remote Access~~

~~19. Organization stance on use of wireless networks~~

~~20. Identification of acceptable authentication methods~~

~~21. Identification of trusted and untrusted resources~~

~~22. Monitoring and logging of ingress and egress at Electronic Access Points~~

~~23. Maintaining up-to-date anti-malware software before initiating Interactive Remote Access~~

~~24. Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access~~

~~25. Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access~~

~~26. For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls~~

~~27. Physical security of BES Cyber Systems (CIP-006)~~

~~28. Strategy for protecting Cyber Assets from unauthorized physical access~~

~~29. Acceptable physical access control methods~~

~~30. Monitoring and logging of physical ingress~~

~~31. System security management (CIP-007)~~

~~32. Strategies for system hardening~~

~~33. Acceptable methods of authentication and access control~~

~~34. Password policies including length, complexity, enforcement, prevention of brute force attempts~~

~~35. Monitoring and logging of BES Cyber Systems~~

~~36. Incident reporting and response planning (CIP-008)~~

~~37. Recognition of Cyber Security Incidents~~

~~38. Appropriate notifications upon discovery of an incident~~

~~39. Obligations to report Cyber Security Incidents~~

~~40. 1.1.6 Recovery plans for BES Cyber Systems (CIP-009)~~

~~41. Availability of spare components~~

~~42. Availability of system backups~~

~~43. 1.1.7 Configuration change management and vulnerability assessments (CIP-010)~~

~~44. Initiation of change requests~~

~~45. Approval of changes~~

~~46. Break-fix processes~~

~~47. 1.1.8 Information protection (CIP-011)~~

~~48. Information access control methods~~

~~49. Notification of unauthorized information disclosure~~

~~50. Information access on a need-to-know basis~~

~~51. 1.1.9 Declaring and responding to CIP Exceptional Circumstances~~

~~52. Processes to invoke special procedures in the event of a CIP Exceptional Circumstance~~

~~53. Processes to allow for exceptions to policy that do not violate CIP requirements~~

~~54. For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:~~

~~55. 1.2.1 Cyber security awareness~~

~~56. Method(s) for delivery of security awareness~~

~~57. Identification of groups to receive cyber security awareness~~

~~58. 1.2.2 Physical security controls~~

~~59. Acceptable approach(es) for selection of physical security control(s)~~

~~60. 1.2.3 Electronic access controls~~

~~61. Acceptable approach(es) for selection of electronic access control(s)~~

~~62. 1.2.4 Cyber Security Incident response~~

~~63. Recognition of Cyber Security Incidents~~

~~64. Appropriate notifications upon discovery of an incident~~

~~65. Obligations to report Cyber Security Incidents~~

~~66. 1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~67. Acceptable use of Transient Cyber Asset(s) and Removable Media~~

~~68. Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media~~

~~69. Method(s) to request Transient Cyber Asset and Removable Media~~

~~70. 1.2.6 Declaring and responding to CIP Exceptional Circumstances~~

~~71. Process(es) to declare a CIP Exceptional Circumstance~~

~~72. Process(es) to respond to a declared CIP Exceptional Circumstance~~

~~73. Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.~~

~~74. In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.~~

~~75.Requirement R2:~~

~~76. The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.~~

~~78.Requirement R2, Attachment 1~~

~~79. As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.~~

~~80. Guidance for each of the subject matter areas of Attachment 1 is provided below.~~

~~81.Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness~~

~~82. The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.~~

~~83. Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.~~

~~84.Requirement R2, Attachment 1, Section 2 – Physical Security Controls~~

~~85. The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located~~

~~within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.~~

86. ~~The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.~~

87. ~~The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.~~

88. ~~Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.~~

89. ~~User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.~~

90.~~Requirement R2, Attachment 1, Section 3 – Electronic Access Controls~~

91. ~~Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.~~

92. ~~When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound~~

~~electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).~~

~~93. When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.~~

~~94. In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.~~

~~95. The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.~~

~~96. Electronic Access Control Exclusion~~

~~97. In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls~~

~~noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.~~

~~98. Considerations for Determining Routable Protocol Communications~~

~~99. To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.~~

~~100. When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.~~

~~101. Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.~~

~~102. Determining Electronic Access Controls~~

~~103. Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and~~

~~implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.~~

~~104.~~ **~~Concept Diagrams~~**

~~105. The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.~~

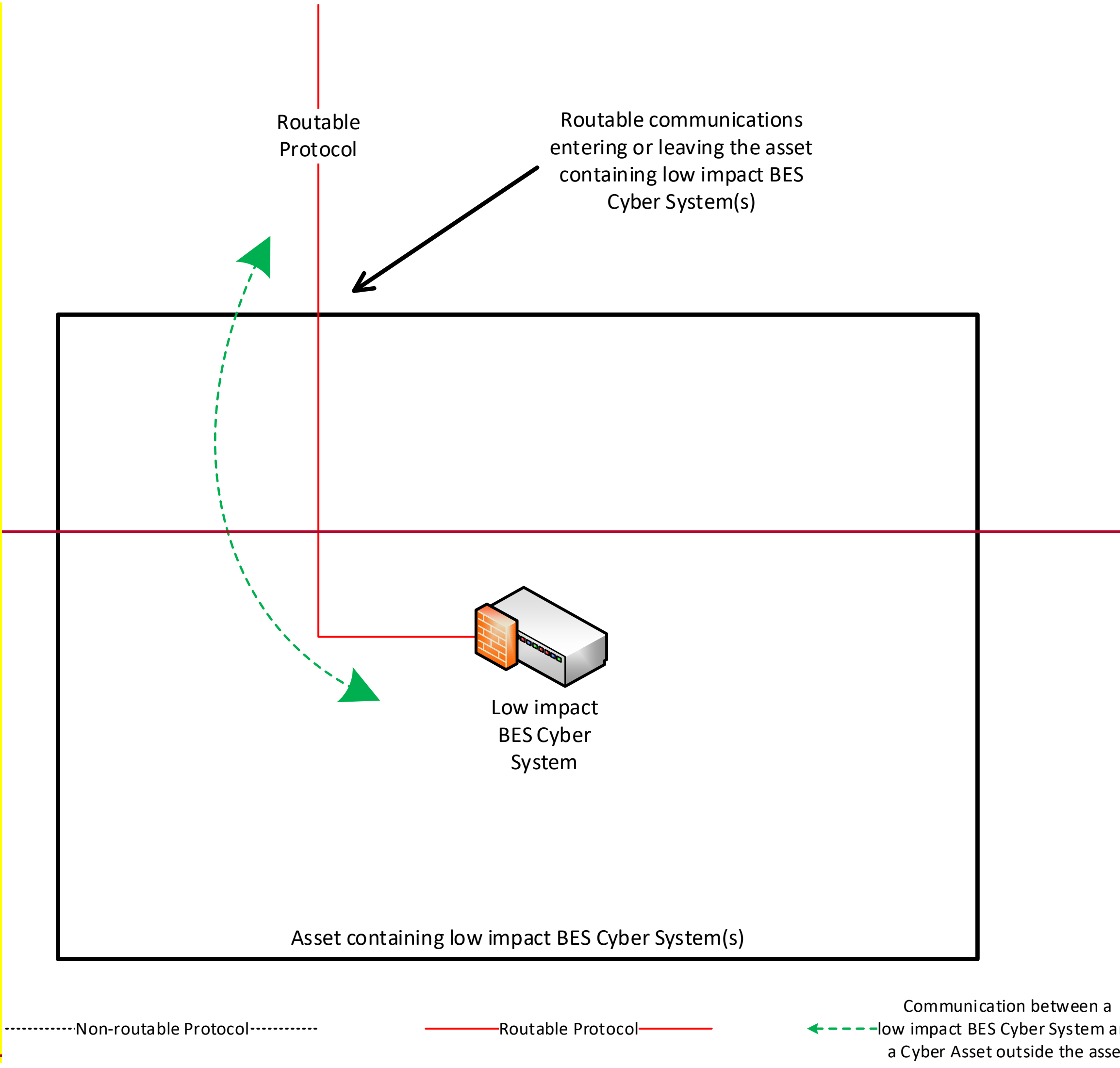
~~106. NOTE:~~

~~107. This is not an exhaustive list of applicable concepts.~~

~~108. The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.~~

~~Reference Model 1 – Host-based Inbound & Outbound Access Permissions~~

~~The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~

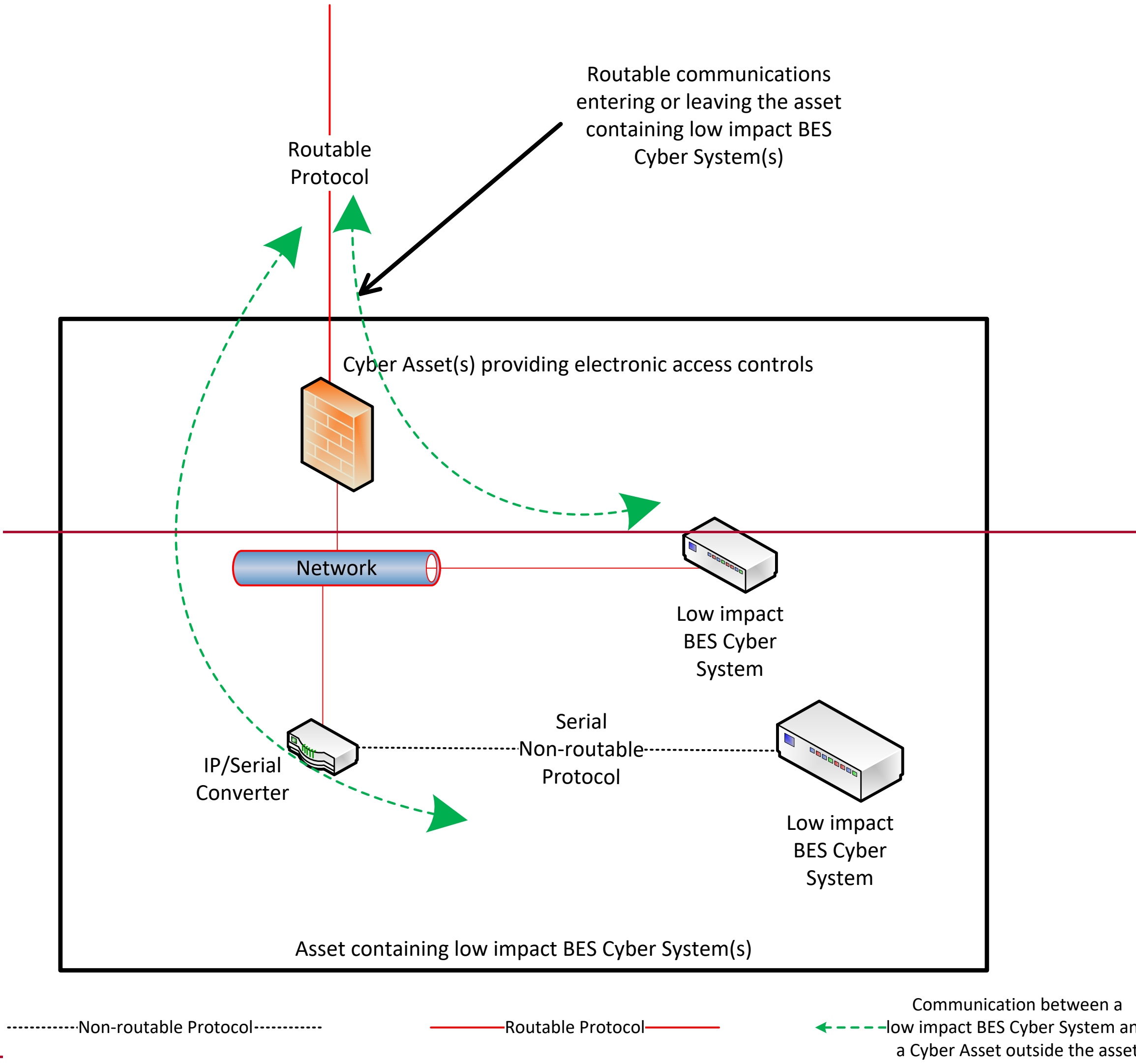


~~109.~~

~~110. Reference Model 1~~

~~111. Reference Model 2 – Network-based Inbound & Outbound Access Permissions~~

~~112. The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~

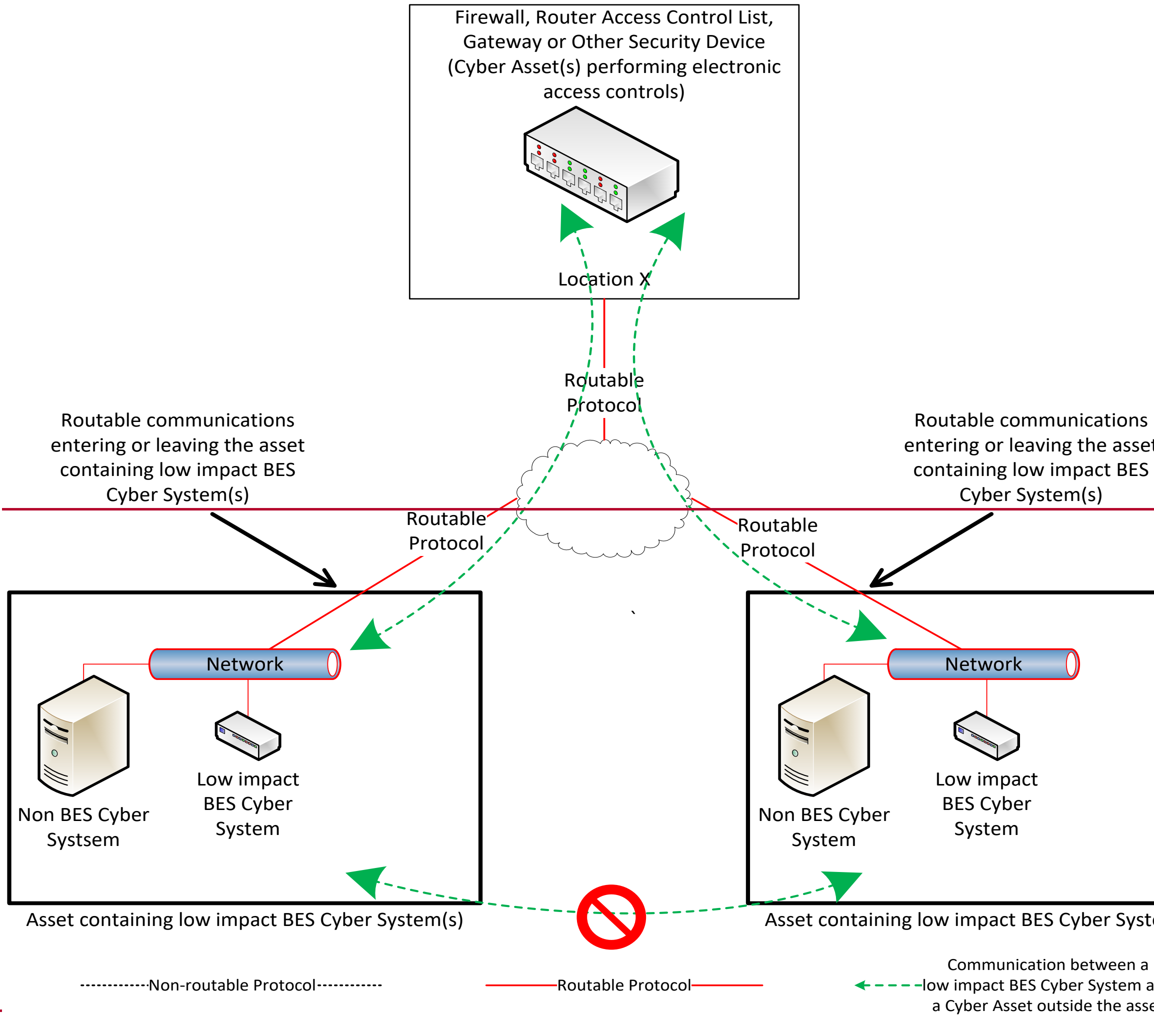


~~113.~~

~~Reference Model 2~~

~~114. Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions~~

~~115. The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).~~

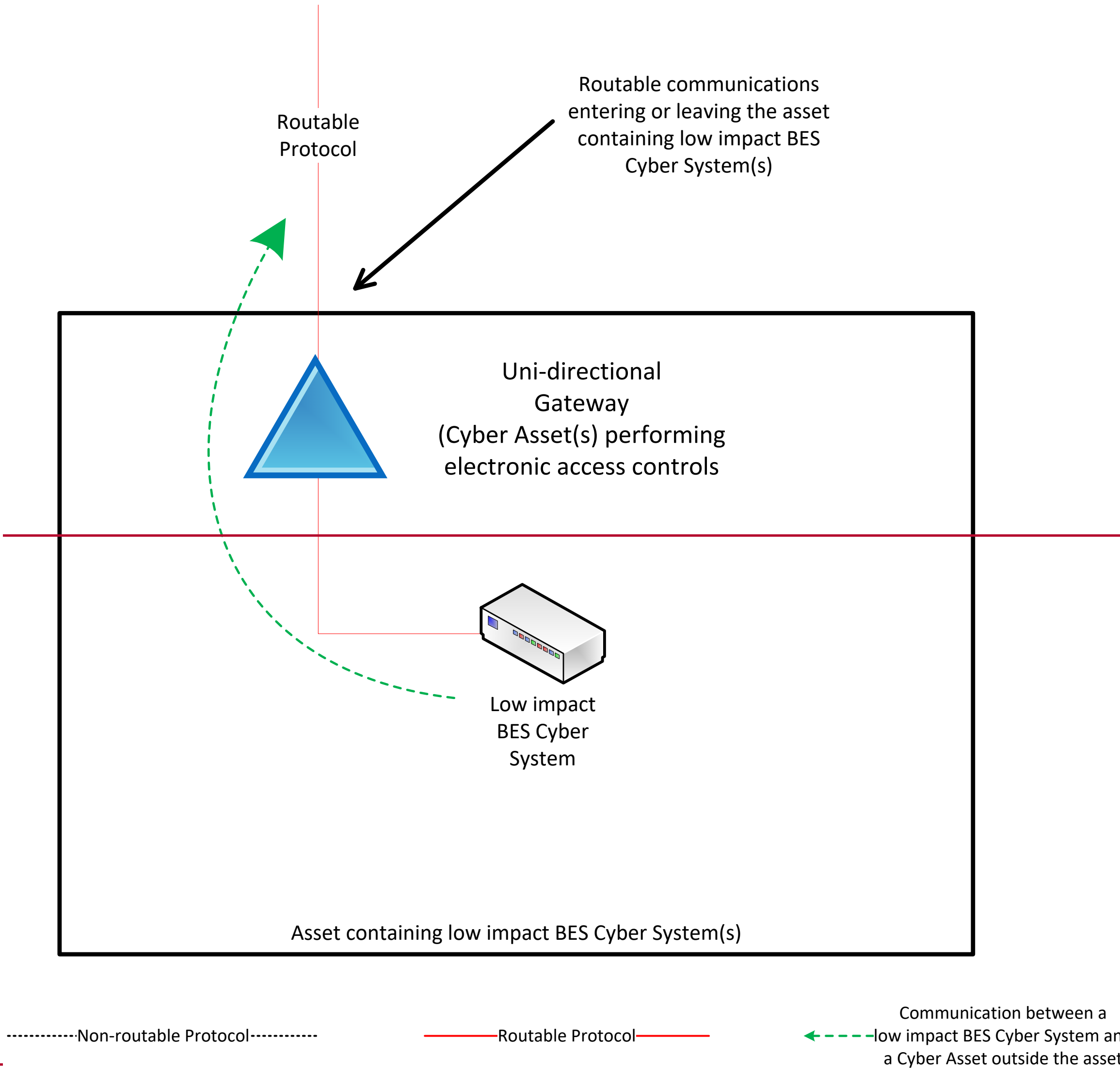


~~116.~~

~~Reference Model 3~~

~~117. **Reference Model 4 – Uni-directional Gateway**~~

~~118. The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.~~

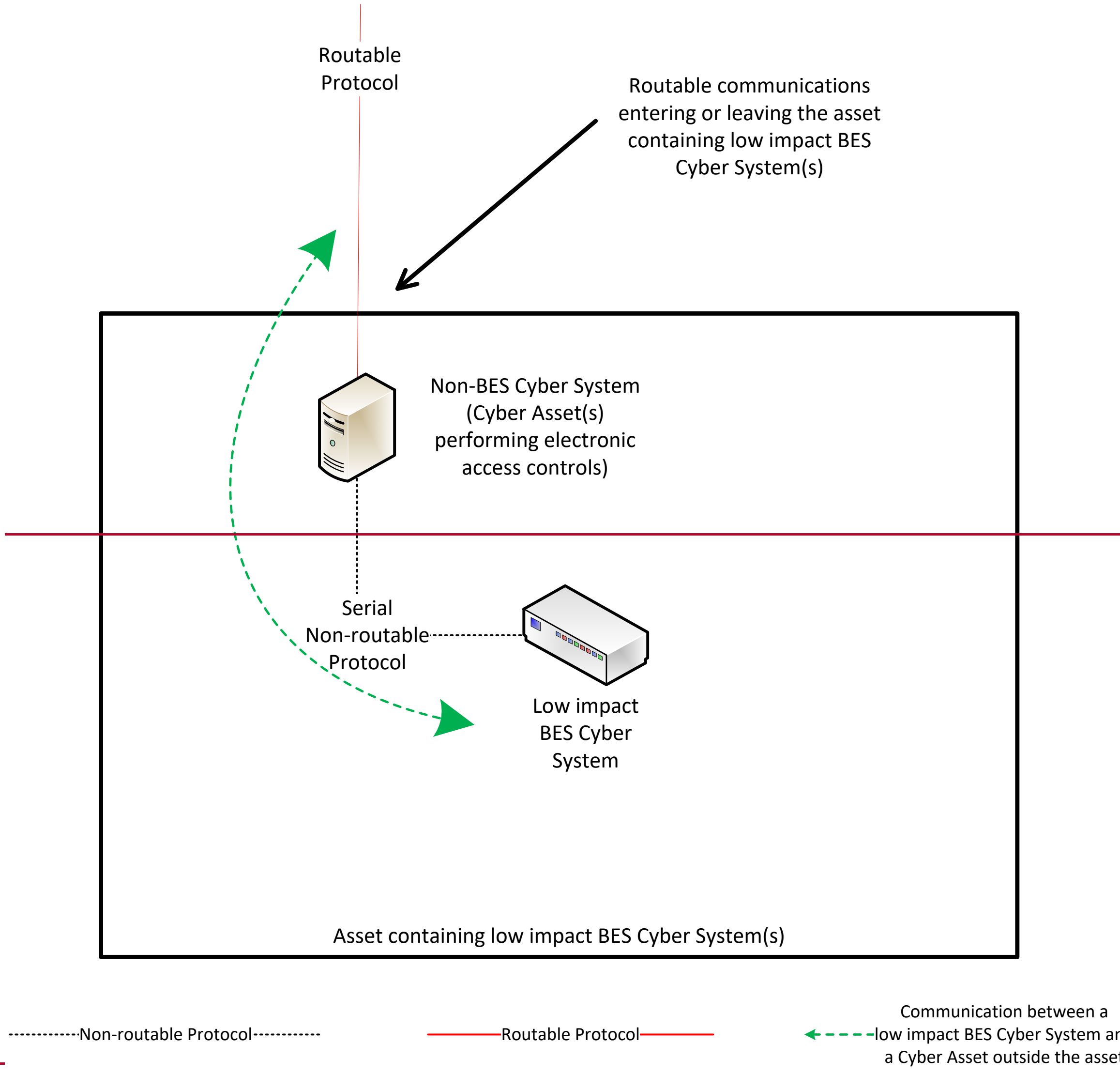


~~119.~~

~~120. Reference Model 4~~

~~121. Reference Model 5 – User Authentication~~

~~122. This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.~~

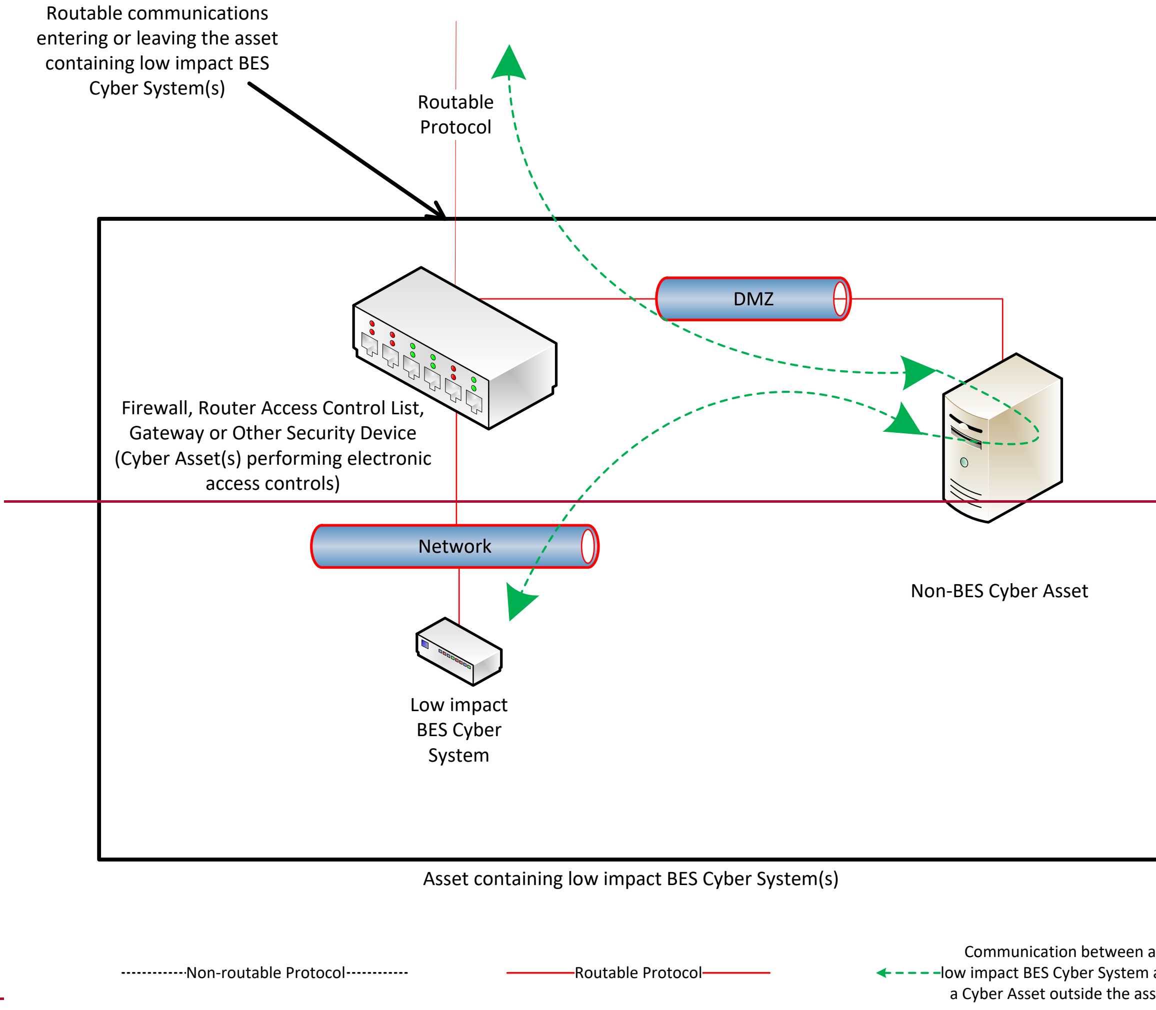


~~123.~~

~~*Reference Model 5*~~

~~124. Reference Model 6 – Indirect Access~~

~~125. In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.~~

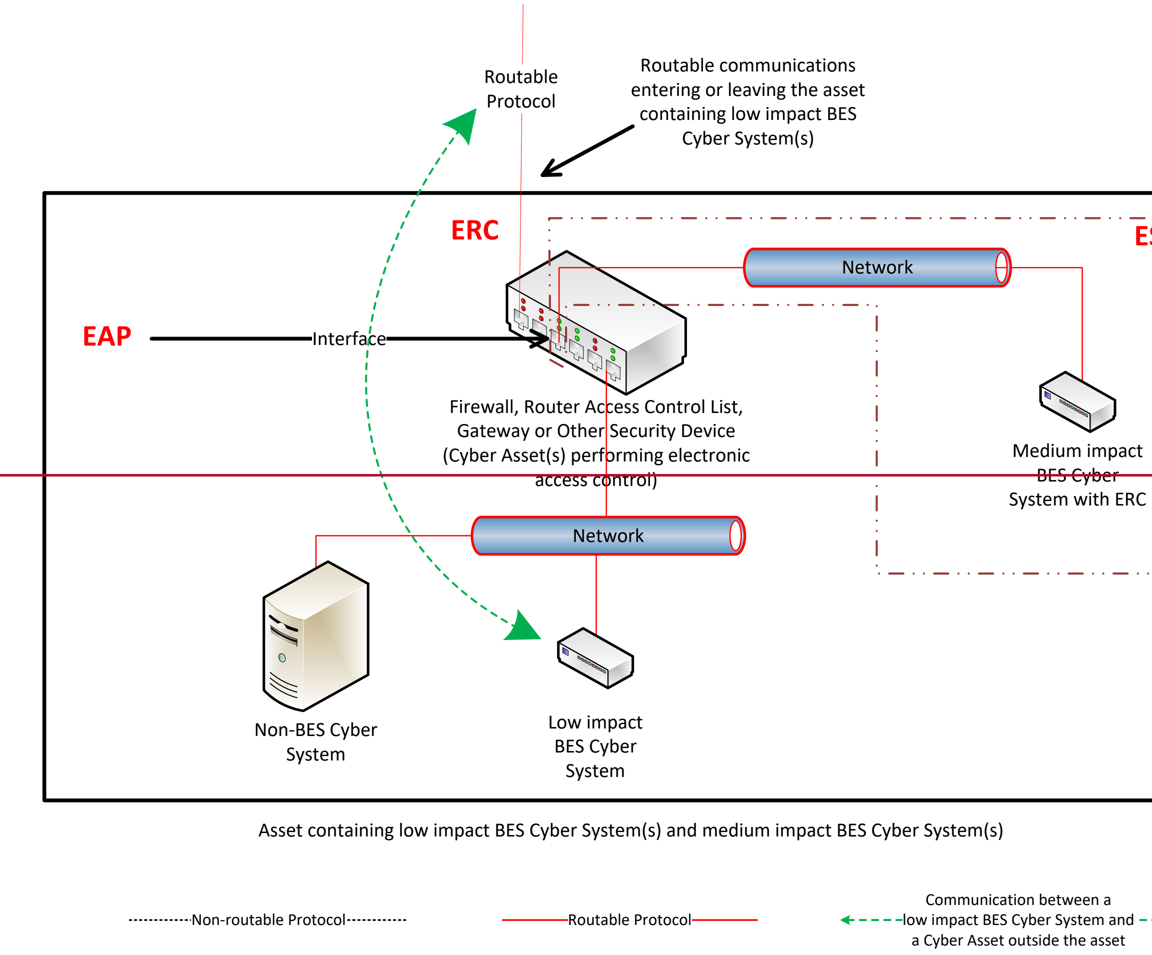


~~126.~~

~~127. Reference Model 6~~

~~128. Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC~~

~~129. In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.~~



~~130. Reference Model 7~~

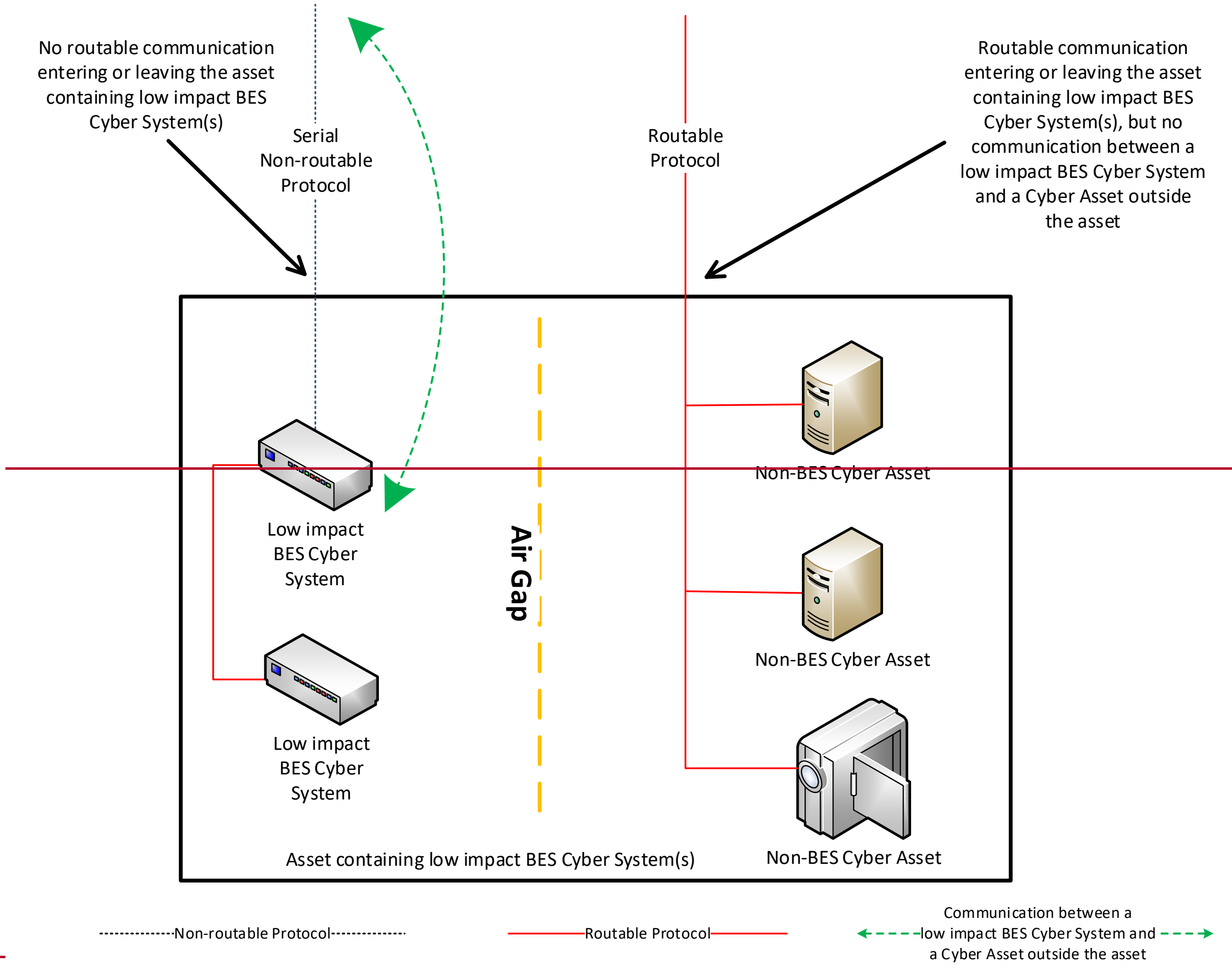
~~131. Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required~~

~~132. In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:~~

~~133. The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;~~

~~134. The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.~~

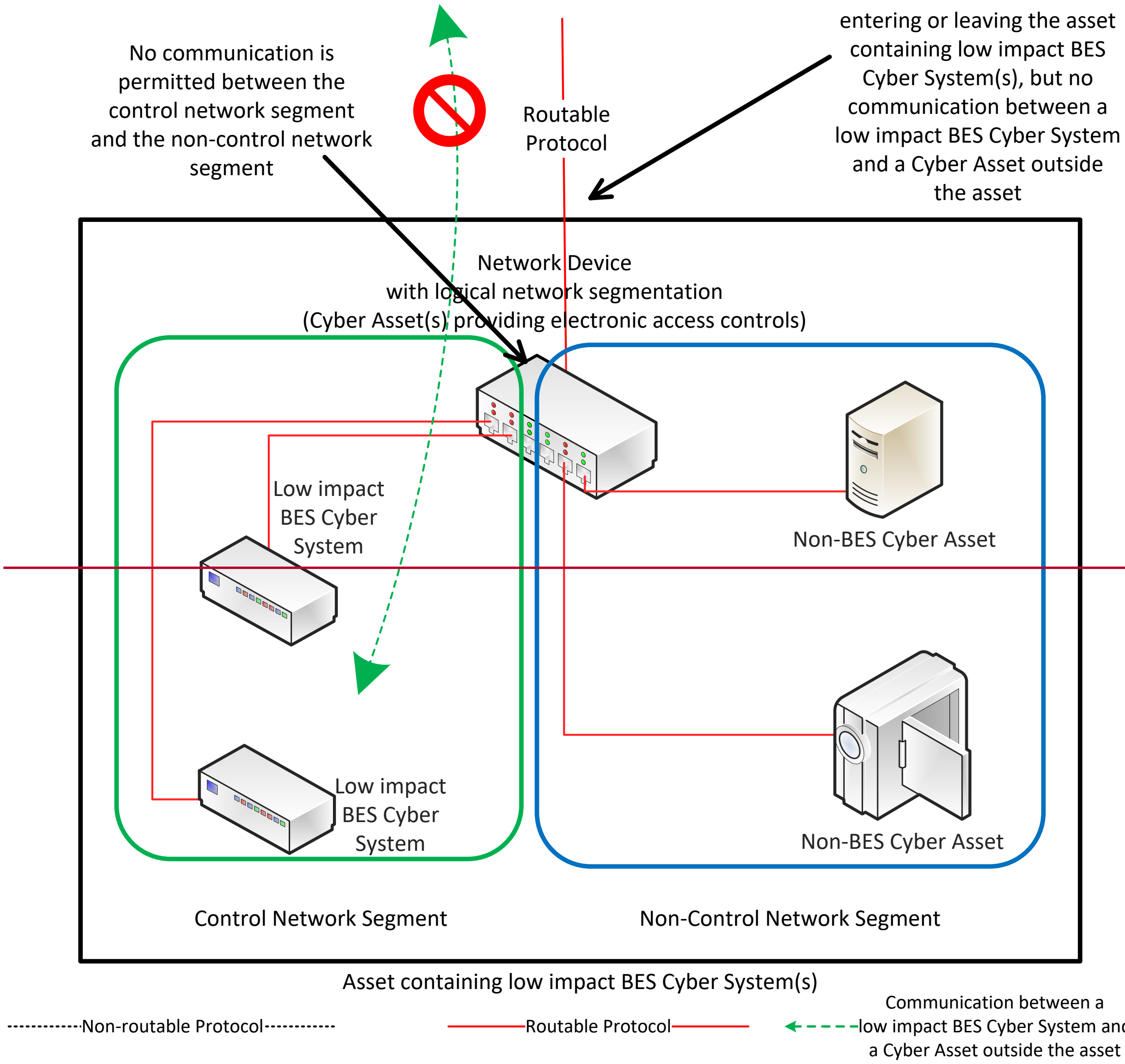
~~135. The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).~~



~~136. Reference Model 8~~

~~137. Reference Model 9 – Logical Isolation - No Electronic Access Controls Required~~

~~138. In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.~~

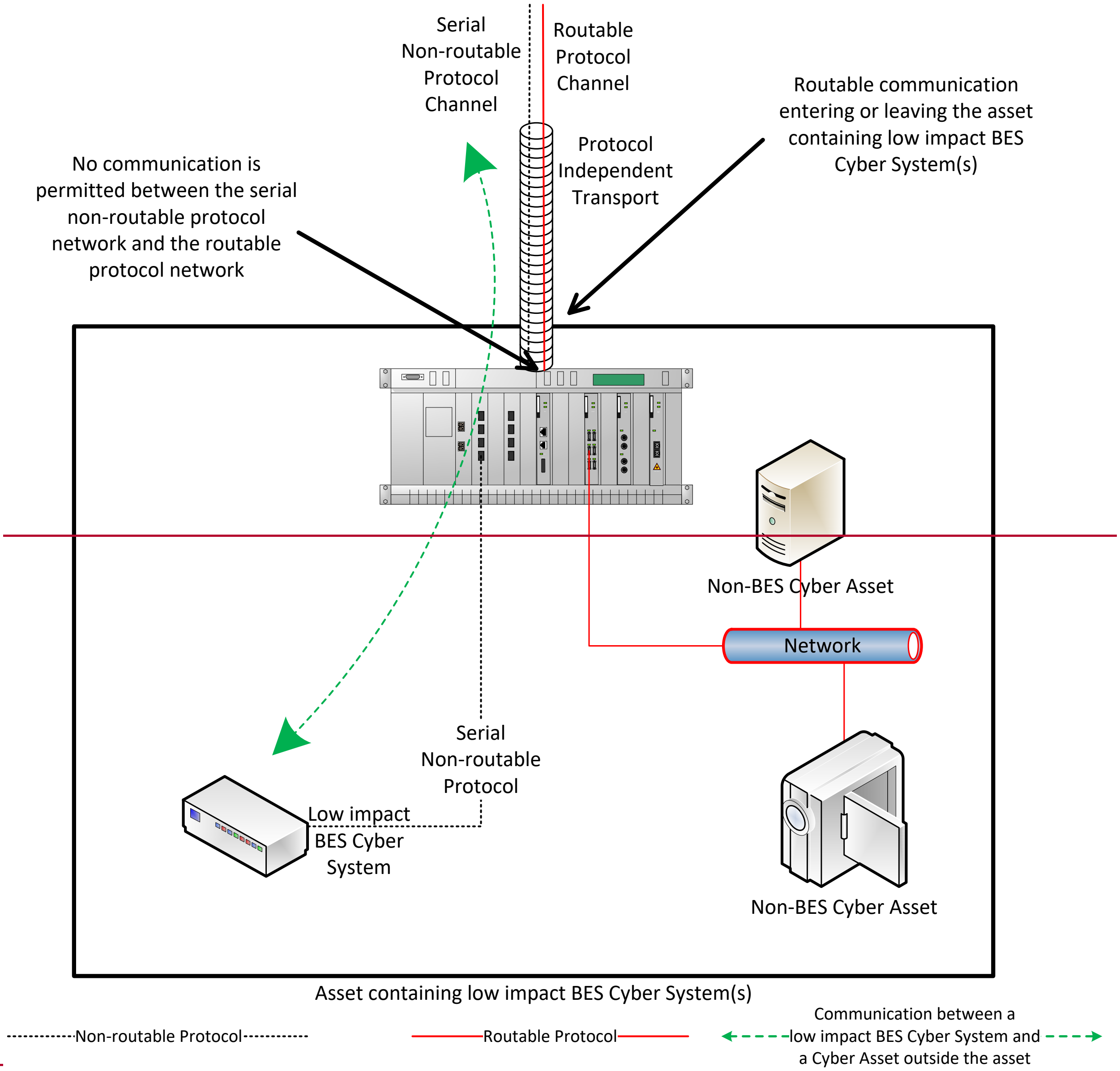


~~139.~~

~~Reference Model 9~~

~~140. Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required~~

~~141. In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.~~



~~142.~~

~~**143.** Reference Model 10~~

~~144. Dial-up Connectivity~~

~~145. Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.~~

~~146. Insufficient Access Controls~~

~~147. Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:~~

~~148. An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.~~

~~149. A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.~~

~~150. Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.~~

~~151. Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response~~

~~152. The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.~~

~~153. Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.~~

~~154. The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise~~

~~as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity's response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.~~

~~155. For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, "A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System." The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.~~

~~156. Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation~~

~~157. Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.~~

~~158. Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~

~~159. Examples of these temporarily connected devices include, but are not limited to:~~

~~160. Diagnostic test equipment;~~

~~161. Equipment used for BES Cyber System maintenance; or~~

~~162. Equipment used for BES Cyber System configuration.~~

~~163. To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.~~

~~164. With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.~~

~~165. Malicious Code Risk Mitigation~~

~~166. The terms "mitigate", "mitigating", and "mitigation" are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.~~

~~167. Per Transient Cyber Asset Capability~~

~~168. As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.~~

~~169. Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity~~

~~170. For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.~~

~~171. **Section 5.1:** Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.~~

~~172. The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.~~

~~173. Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity~~

~~may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~174. The following is additional discussion of the methods to mitigate the introduction of malicious code.~~

~~175. Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.~~

~~176. Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.~~

~~177. When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.~~

~~178. If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.~~

~~179. Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity~~

~~180. Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient~~

~~Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.~~

~~181. To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.~~

~~182. **Section 5.2.1:** Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.~~

~~183. Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.~~

~~184. Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.~~

~~185. Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.~~

~~186. Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.~~

~~187. Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.~~

~~**188.** **Section 5.2.2:** The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact~~

~~[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014~~

~~BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.~~

~~189.~~

~~190. Requirement R2, Attachment 1, Section 5.3 - Removable Media~~

~~191. Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.~~

~~192. **Section 5.3:** Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.~~

~~193. As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.~~

~~194. Requirement R3:~~

~~195. The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.~~

~~196. Requirement R4:~~

~~197. As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership~~

~~for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.~~

~~198. The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.~~

~~200. Rationale:~~

~~201. During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~202. Rationale for Requirement R1:~~

~~203. One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.~~

~~204. Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.~~

~~205. Rationale for Requirement R2:~~

~~206. In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~207. Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.~~

~~208. Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.~~

~~209. Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):~~

~~210. Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."~~

~~211. The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".~~

~~212. The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.~~

~~213. Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.~~

~~214. Rationale for Section 5 of Attachment 1 (Requirement R2):~~

~~215. Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES~~

~~through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.~~

~~216. Rationale for Requirement R3:~~

~~217. The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.~~

~~218. FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.~~

~~219. Rationale for Requirement R4:~~

~~220. The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.~~

~~221.~~3. ~~In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-8

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **"Applicable Systems":** Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R1 – Security Awareness Program

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Part	If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Examples of evidence may include, but are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High impact BCS and their associated EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part	Examples of evidence may include, but are not limited to, workflow or sign-off form showing access removal for any individual

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part	5.1) within 30 calendar days of the effective date of the termination action.	BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For termination actions, remove the individual’s ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	authorized unescorted physical access. (Part 2.2) OR The Responsible Entity did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for two individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1)	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)
R5	The Responsible Entity did not revoke individual's user accounts upon termination action within 30 calendar days of the date of	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	termination action for one or more individuals. (Part 5.3) OR The Responsible Entity did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	within 24 hours of the termination action for one individual. (Part 5.1) OR The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	complete the removal within 24 hours of the termination action for two individuals. (Part 5.1) OR The Responsible Entity for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action for three or more individuals. (Part 5.1) OR The Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (Requirement R6) OR The Responsible Entity, for four or more individuals, did not authorize provisioned electronic access to

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not perform the verification required by Part 6.2 within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for one individual, did not remove the individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for two individuals, did remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for three individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for four or more individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the third draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53~~45~~-day formal comment period with ballot	February 18 – April ~~4~~12, 2022
45-day formal comment period with ballot	August 10 – September 30, 2022

Anticipated Actions	Date
Final Ballot	~~April~~ October 2022
Board adoption	~~May~~ November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 4~~3~~ Definitions”

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-8

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R1 – Security Awareness Program

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Part	If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Examples of evidence may include, but are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.
5.3	High impact BCS and their associated EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part	Examples of evidence may include, but are not limited to, workflow or sign-off form showing access removal for any individual

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part	5.1) within 30 calendar days of the effective date of the termination action.	BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: - List of authorized individuals; - List of individuals who have been provisioned access; - Verification that provisioned access is appropriate based on need; and - Documented reconciliation actions, if any.
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Version History

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train four or more individuals (with the exception of CIP Exceptional

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3)

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	for one individual. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	3.2.2 for two individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	OR The Responsible Entity did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active	The Responsible Entity did not authorize electronic access or	The Responsible Entity did not authorize electronic	The Responsible Entity did not implement any documented

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	unescorted physical access based on need for one individual. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	access or unescorted physical access based on need for two individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	program(s) for access management. (Requirement R4) OR The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity did not revoke individual's user accounts upon termination action within 30 calendar days of the date of termination action for one or more individuals. (Part 5.3) OR The Responsible Entity did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action for one individual. (Part 5.1) OR The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal within 24 hours of the termination action for two individuals. (Part 5.1) OR The Responsible Entity for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action for three or more individuals. (Part 5.1) OR The Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity, for one individual, did not authorize provisioned electronic access to	The Responsible Entity, for two individuals, did not authorize provisioned electronic access	The Responsible Entity, for three individuals, did not authorize provisioned	The Responsible Entity did not implement one or more documented

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for one individual, did not remove the individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for two individuals, did remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 within 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for three individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	access management program(s) for BCSI. (Requirement R6) OR The Responsible Entity, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for four or more individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April-12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-8~~7~~

3. Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting ~~BES Cyber Systems~~BCS.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-8~~7~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~**4.2.3.2.**~~**4.2.3.3.** Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002~~-75.1a~~ identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan” ~~for CIP-004-7~~.

~~**Background:** Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *“Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].”* The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple~~

~~high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**"Applicable Systems" Columns in Tables:**~~
~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8~~7~~ Table R1 – Security Awareness Program

Part	Applicable Systems	Requirements	Measures
1.1	High ~~I~~impact ~~BES Cyber Systems~~BCS Medium ~~I~~impact ~~BES Cyber Systems~~BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to ~~BES Cyber~~Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8~~7~~ Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8~~7~~ Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8~~7~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~I~~impact ~~BES Cyber Systems~~BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for ~~BES Cyber Systems~~BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a ~~BES Cyber System's~~BCS electronic interconnectivity and	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-8~~7~~ Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
		interoperability with other Cyber ~~Assets~~System, including Transient Cyber Assets (TCA), and with Removable Media.	
2.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to ~~a~~Applicable Systems~~Cyber Assets~~, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

CIP-004-8~~7~~ Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS SCI supporting an Applicable System in this Part		

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to ~~BES Cyber Systems~~ Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8~~7~~ Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~8~~7 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium iImpact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated:	Criteria or process for verifying that personnel risk assessments performed	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation

CIP-004-8~~7~~ Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.
3.5	High iImpact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 ~~to~~ through 3.4 within the last seven years.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8~~7~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP).	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a ~~Physical Security Perimeter~~PSP.
4.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium iImpact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated:	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of

CIP-004-8~~7~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part		personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by

CIP-004-8~~7~~ Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8~~7~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	A process to initiate removal of an individual’s ability for unescorted physical access and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and	For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is

CIP-004-8~~7~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS SCI supporting an Applicable System in this Part		not necessary.
5.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the

CIP-004-8~~7~~ Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
		circumstances.	operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the ~~“~~Applicable Systems~~”~~ identified in *CIP-004-8~~7~~ Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8~~7~~ Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8~~7~~ Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8~~7~~ Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1~~.~~) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8~~7~~ Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: - List of authorized individuals; - List of individuals who have been provisioned access; - Verification that provisioned access is appropriate based on need; and - Documented reconciliation actions, if any.
6.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. **Compliance Enforcement Authority:** “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

   1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
   - The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security~~	The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR	The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include four or more of the

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~training program but failed to~~did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~ did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. –(Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity ~~has a program for conducting~~	The Responsible Entity ~~has a program for conducting~~	The Responsible Entity ~~has a program for conducting~~	The Responsible Entity did not have all of the required elements

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~ personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year~~	~~Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the personnel risk assessments~~PRA~~ as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR	~~Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the personnel risk assessments~~PRA~~ as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR	as described by 3.1 through 3.4 included within documented program(s) for implementing ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the personnel risk assessments~~PRA~~ as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including~~

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~ through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR	The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~ through 3.2.2 for two individuals. (Parts 3.2 & 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4)	The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~ through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate criminal history records check for access authorization for three	~~contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~ through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity ~~did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not evaluate

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not conduct ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~ for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments~~PRA~~ completion date. (Part 3.5)	OR The Responsible Entity did not conduct ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~ for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments~~PRA~~ completion date. (Part 3.5)	individuals. (Parts 3.3 ~~&~~through 3.4) OR The Responsible Entity did not conduct ~~P~~personnel ~~R~~risk ~~A~~assessments ~~(PRAs)~~ for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments~~PRA~~ completion date. (Part 3.5)	criminal history records check for access authorization for four or more individuals. (Parts 3.3 ~~&~~through 3.4) OR The Responsible Entity did not conduct ~~P~~personnel ~~R~~risk ~~A~~assessments~~(PRAs)~~ for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments~~PRA~~ completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR ~~The Responsible Entity did not implement one or more documented program(s) for access management that includes a process to authorize electronic access or unescorted physical access. (4.1)~~

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity ~~has implemented processes to~~ did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for 5% or less of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. ~~-~~(Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 5% but less than (or equal to) 10% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. ~~-~~(Part 4.3)	records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 10% but less than (or equal to) 15% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 15% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity ~~has implemented one or more process(es) to~~did not revoke ~~the~~ individual's user accounts upon termination action ~~but did not do so for~~ within 30 calendar days of the date of termination action for one or more individuals. (Part 5.3) OR The Responsible Entity ~~has implemented one or more process(es) to~~ did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer~~, but did not do so for~~ within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity ~~has implemented one or more~~	The Responsible Entity ~~has implemented one or more process(es) to~~did not initiate removal~~e~~ of the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for one individual. (Part 5.1) OR The Responsible Entity ~~has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~ for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day	The Responsible Entity ~~has implemented one or more process(es) to~~did not initiate removal~~e~~ of the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for two individuals. (Part 5.1) OR The Responsible Entity ~~has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~ for two individuals, did not revoke the authorized electronic access to individual	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity ~~has implemented one or more process(es) to~~did not initiate removal~~e~~ of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for three or more individuals. (Part 5.1) OR The Responsible Entity ~~has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~ for three or more individuals, did not revoke the authorized electronic

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but~~ did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	following the predetermined date. (Part 5.2)	accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. -(Part 6.1) OR The Responsible Entity did not perform~~ed~~ the verification required by ~~Requirement R6~~	The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform~~ed~~ the verification required by	The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform~~ed~~ the verification required by	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (Requirement R6) OR The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or

R #	Violation Severity Levels (CIP-004-8~~7~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Part 6.2 ~~more than~~within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for one individual, did not remove the individual's ability to use provisioned access to BCSI ~~do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	~~Requirement R6~~ Part 6.2 ~~more than~~within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for two individuals, did remove ~~the~~each individual's ability to use provisioned access to BCSI ~~not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	~~Requirement R6~~ Part 6.2 within ~~more than~~ 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for three individuals, did not remove each individual's ability to use provisioned access to BCSI~~do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform~~ed~~ the verification required by ~~Requirement R6~~ Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to remove the individual's ability to use provisioned access to BCSI but~~, for four or more individuals, did not ~~do~~ remove ~~the~~each individual's ability to use provisioned access to BCSI ~~so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-8
3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**

    4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. **Balancing Authority**

    4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. **Generator Operator**

    4.1.4. **Generator Owner**

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP.	Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Systems connected via a routable protocol within each ESP.
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Physical isolation of an ESP; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that enforce an ESP for an Applicable System in Part 1.1	Permit only needed routable protocol communications to and from Management Interfaces of Applicable Systems, and deny all other routable protocol communications, per system capability.	Examples of evidence may include, but are not limited to, documentation of the access enforcement configuration or settings to or from the Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the management plane resources (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).
1.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
			layer firewall, etc.) are implemented.
1.6	High impact BCS and their associated PCA Medium impact BCS at Control Centers and their associated PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time-sensitive communication of Protection Systems.	Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Permit authorized Interactive Remote Access (IRA), if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	Intermediate Systems used to access an Applicable System in Part 2.1	Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Examples of evidence may include, but are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption) initiate and terminate.
2.3	Intermediate System used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for all IRA.	Example of evidence may include, but are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID;

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			- Something the individual has such as tokens, digital certificates, or smart cards; or - Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
2.4	High impact BCS with vendor remote access and their associated PCA Medium impact BCS with vendor remote access and their associated PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, including IRA and system-to-system remote access, such as: - Methods for accessing logged or monitoring information to determine active vendor remote access sessions; - Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or - Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High impact BCS with vendor remote access and their associated PCA Medium impact BCS with vendor remote access and their associated PCA SCI supporting an Applicable System in this Part	Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access • (including IRA and system-to-system remote access).
2.6	Intermediate System used to access an Applicable System in Part 2.1	Intermediate Systems shall: 2.6.1. Not share CPU or memory resources with any part of a high or medium impact BCS; and 2.6.2. Restrict their routable protocol communications to BCS and their associated PCAs through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*.

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with high impact BCS EACMS and PACS associated with medium impact BCS with ERC SCI supporting an Applicable System in this Part	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with high impact BCS EACMS and PACS associated with medium impact BCS with ERC SCI supporting an Applicable System in this Part	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	Applicable Systems	Requirements	Measures
			firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the ESP required by Part 1.6.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not protect the Applicable Systems connected to the network with routable protocol with an ESP. (Part 1.1) OR The Responsible Entity did not permit only needed communications to and from Applicable Systems either individually or as a group and deny all other communications. (Part 1.2) OR The Responsible Entity did not permit only needed and controlled communications to and from Management Interfaces for Applicable Systems and deny all other communications. (Part 1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to span a single ESP between PSPs, as required by Part 1.3. OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the Applicable Systems. (Part 1.5)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access (including IRA and system-to-system remote access)	The Responsible Entity did not implement processes for three of the applicable Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(Part 2.5).	access (including IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not ensure routable protocol communications are through an ESP as required by Part 2.6.
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI*. (Requirement R3)	The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for EACMS or SCI supporting EACMS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS or SCI supporting EACMS (Part 3.2).	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI*. (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~third~~ Fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53~~45~~-day formal comment period with ballot	February 18 – April 12~~4~~, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	~~April~~ October 2022
Board adoption	~~May~~ November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified new terms titled "Project 2016-02 Draft 4~~3~~ Definitions"

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-8
3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems”: Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP.	Examples of evidence may include, but is not limited to, ~~-~~a list of all ESPs with all uniquely identifiable applicable Cyber ~~Assets~~ Systems connected via a routable protocol within each ESP.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, and deny all other routable protocol communications, through the ESP;~~,~~ excluding time-sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Physical isolation of an ESP; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting an Applicable System from Part 1.1~~.~~ EACMS, and their supporting SCI, that enforce an ESP for an Applicable System in Part 1.1	Permit only needed routable protocol communications to and from Management Interfaces of Applicable Systems, and deny all other routable protocol communications, per system capability.	Examples of evidence may include, but are not limited to, documentation of the access enforcement configuration or settings to or from the Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the management plane resources (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~1.4~~	~~High impact BCS and their associated PCA~~ ~~Medium impact BCS at Control Centers and their associated PCA~~	~~Protect the data traversing communication links used to span a single ESP between PSPs through the use of:~~ ~~• Confidentiality and integrity controls (such as encryption), or~~ ~~• Physical controls that restrict access to the cabling and other non programmable communication components in those instances when such cabling and components are located outside of a PSP,~~ ~~Excluding:~~ ~~i. Real time Assessment and Real time monitoring data while being transmitted between Control Centers subject to CIP 012; and~~ ~~ii. Time sensitive communication of Protection Systems.~~	~~Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as:~~ ~~• Configurations or settings used to enforce encryption; or~~ ~~• The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).~~
1.4	High impact BCS ~~with Dial-up Connectivity~~ and their associated PCA Medium impact BCS ~~with Dial-up Connectivity~~ and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, If any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.
~~1.6~~	~~High impact BCS~~ ~~Medium impact BCS at Control Centers~~	~~Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.~~	~~An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.~~

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High impact BCS and their associated PCA Medium impact BCS at Control Centers and their associated PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time-sensitive communication of Protection Systems.	Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Permit authorized Interactive Remote Access (IRA), if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	Intermediate Systems used to access an Applicable Systems ~~of~~in Part 2.1	~~For all IRA, p~~Protect the confidentiality and integrity ~~(e.g., encryption)~~ of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Examples of evidence may include, but are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption) initiate and terminate.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	Intermediate System used to access an Applicable Systems ~~of~~in Part 2.1	~~For all IRA, r~~Require multi-factor authentication to the Intermediate System for all IRA.	Example of evidence may include, but are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-8 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.4	High impact BCS with vendor remote access and their associated PCA Medium impact BCS with vendor remote access and their associated PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions, ~~(~~including IRA and system-to-system remote access~~)~~.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, ~~(~~including IRA and system-to-system remote access~~)~~, such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High impact BCS with vendor remote access and their associated PCA Medium impact BCS with vendor remote access and their associatedPCA SCI supporting an Applicable System in this Part	Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access, ~~(~~including IRA and system-to-system remote access~~)~~.
2.6	Intermediate System used to access an Applicable Systems in~~of~~ Part 2.1	Intermediate Systems shall: 2.6.1. Not share CPU or memory resources with any part of a high or medium impact BCS; and 2.6.2. Restrict their routable protocol communications to BCS and their associated PCAs through an ESP. ~~Routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.~~	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with High impact BCS EACMS and PACS associated with Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High impact BCS EACMS and PACS associated with Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account;

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	Applicable Systems	Requirements	Measures
			disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority:** "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving the ESP required by Part 1.6.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not protect the Applicable Systems connected to the network with routable protocol with an ESP. (Part 1.1) OR The Responsible Entity did not permit only needed communications to and from Applicable Systems either individually or as a group and deny all other communications. (Part 1.2) OR The Responsible Entity did not permit only needed and controlled communications to and from Management Interfaces for Applicable Systems and deny all other communications. (Part 1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to span a single ESP between PSPs, as required by Part 1.3. OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the Applicable Systems. (Part 1.5)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access	The Responsible Entity did not implement processes for three of the applicable Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(including IRA and system-to-system remote access) (Part 2.5).	access (including IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not ensure routable protocol communications are through an ESP as required by Part 2.6.
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI*. (Requirement R3)	The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for EACMS or SCI supporting EACMS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS or SCI supporting EACMS (Part 3.2). ~~OR~~	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI*. (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for SCI supporting PACS and EACMS (Part 3.1).~~ ~~OR~~ ~~The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for SCI supporting PACS and EACMS (Part 3.2).~~	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 –September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-8~~7~~

3. **Purpose:** To ~~manage electronic access to~~ protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of ~~by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to~~ misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8~~7~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.5.**~~**4.2.3.6.** Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See ~~Implementation Plan for~~ "Project 2016~~9~~-02~~3~~ Modifications to CIP Standards Implementation Plan".

~~**6. Background:** Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~
- ~~**High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.~~

- ~~**High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~
- ~~**Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~ PCA	~~All a~~Applicable Systems ~~Cyber Assets~~ connected to a network via a routable protocol must be protected by an ~~shall reside within a defined~~ ESP.	~~An e~~Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber ~~Assets~~ Systems connected via a routable protocol within each ESP.

CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.2	High ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated~~:~~ PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated~~:~~ PCA	Permit only needed routable protocol communications, and deny all other routable protocol communications, through the ESP; excluding time-sensitive communications of Protection Systems. ~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~	~~An e~~Examples of evidence may include, but ~~is~~are not limited to, documentation that includes the configuration of system and documented reason, such as: ~~network diagrams showing all external routable communication paths and the identified EAPs.~~ • Electronic Access Point (EAP) configuration; • Physical isolation of an ESP; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting an Applicable System from Part 1.1 EACMS, and their supporting SCI, that enforce an ESP for an Applicable System in Part 1.1 ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	Permit only needed routable protocol communications to and from Management Interfaces of Applicable Systems, and deny all other routable protocol communications, per system capability. ~~Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.~~	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation of the access enforcement configuration or settings to or from the Management Interfaces, including documented reasons such as: ~~a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.~~ • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the management plane resources (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).

CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~1.4~~	~~High Impact BES Cyber Systems with Dial-up Connectivity and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated:~~ ~~• PCA~~	~~Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.~~	~~An example of evidence may include, but is not limited to, documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.~~
1.4~~5~~	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part ~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers~~	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability. ~~Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.~~	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, configuration, settings, or ~~documentation~~ documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection. ~~that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.~~
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

CIP-005-8~~7~~ Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.6	High impact BCS and their associated PCA Medium impact BCS at Control Centers and their associated PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time-sensitive communication of Protection Systems.	Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, ~~where technically feasible~~per system capability, in *CIP-005-8~~7~~ Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8~~7~~ Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated~~:~~ PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS ~~with External Routable Connectivity~~ and their associated ~~:~~ PCA SCI supporting an Applicable System in this Part	Permit authorized Interactive Remote Access (IRA), if any, only through an Intermediate System. ~~For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~	Examples of evidence may include, but are not limited to, network diagrams, ~~or~~ architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	Intermediate Systems used to access an Applicable Systems in Part 2.1 ~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~	~~For all Interactive Remote Access~~ IRA, Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System. ~~sessions, utilize encryption that terminates at an Intermediate System.~~	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, architecture documents, configuration or settings detailing where confidentiality and ~~encryption~~integrity controls (e.g., encryption) initiate~~s~~ and terminate~~s~~.

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	• ~~PCA~~		
2.3	Intermediate System used to access an Applicable Systems in Part 2.1 ~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~• PCA~~ •	Require multi-factor authentication ~~for all Interactive Remote Access sessions~~, to the Intermediate System for all IRA.	~~An e~~Example of evidence may include, but are~~is~~ not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High ~~I~~impact ~~BES Cyber Systems~~BCS with vendor remote access and their associated~~:~~ ~~•~~ PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with vendor remote access ~~with External Routable Connectivity~~ and their associated~~:~~ ~~•~~PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions, ~~(~~including ~~Interactive Remote Access~~IRA and system-to-system remote access~~)~~.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, ~~(~~including ~~Interactive Remote Access~~ IRA and system-to-system remote access~~)~~, such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-8~~7~~ Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High ~~I~~impact ~~BES Cyber Systems~~BCS with vendor remote access and their associated~~:~~ PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~vendor remote access and their associated~~:~~ PCA SCI supporting an Applicable System in this Part	Have one or more method(s) to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access).~~,~~ ~~such as:~~ ~~Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or~~ • ~~Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~
2.6	Intermediate System used to access an Applicable System in Part 2.1	Intermediate Systems shall: 2.6.1. Not share CPU or memory resources with any part of a high or medium impact BCS; and 2.6.2. Restrict their routable protocol communications to BCS and their associated PCAs through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8~~7~~ Table R3 –Vendor Remote Access Management for EACMS,~~ and~~ PACS, and SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*.

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS,~~ and~~ PACS, and SCI

Part	Applicable Systems	Requirements	Measures
3.1	EACMS and PACS associated with High ~~I~~impact ~~BES Cyber Systems~~BCS EACMS and PACS associated with Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC SCI supporting an Applicable System in this Part	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with High ~~I~~impact ~~BES Cyber Systems~~BCS EACMS and PACS associated with Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ ERC SCI supporting an Applicable System in this Part	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in

CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS, ~~and~~ PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
			a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious ~~communications for both inbound and outbound~~ Internet Protocol (IP) communications entering or leaving the ESP required by Part 1.6. ~~(1.5)~~	The Responsible Entity did not document one or more processes for *CIP-005-8~~6~~ Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not protect the Applicable Systems connected to the network with routable protocol with an ESP. (Part 1.1) OR ~~The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1)~~ OR The Responsible Entity did not permit only needed communications to and from Applicable Systems either individually or as a

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				group and deny all other communications. (Part 1.2) OR The Responsible Entity did not permit only needed and controlled communications to and from Management Interfaces for Applicable Systems and deny all other communications. (Part 1.3) OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to span a single ESP between PSPs, as required by Part 1.3. OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the Applicable Systems. (Part 1.5) ~~External Routable Connectivity through the~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~ESP was not through an identified EAP. (1.2)~~ ~~OR~~ ~~The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)~~ ~~OR~~ ~~The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)~~
R2.	The Responsible Entity does not have documented processes for one or more of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions	The Responsible Entity did not implement processes for three of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			(including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5).	~~Interactive Remote Access~~ IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not ensure routable protocol communications are through an ESP as required by Part 2.6.
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8~~7~~ Table R3 – Vendor Remote Access Management for EACMS,~~ and~~ PACS, and SCI*. (Requirement R3)	The Responsible Entity ~~had method(s) as required by Part 3.1 for EACMS but~~ did not have a method to determine authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by~~	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity ~~had method(s) as required by Part 3.1 for PACS but~~ did not have a method to determine authenticated vendor-initiated remote	The Responsible Entity did not implement any processes for *CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS,~~ and~~ PACS, and SCI*. (Requirement R3) OR The Responsible Entity did not have any methods as

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		~~Part 3.2 for EACMS but~~ did not have a method to terminate authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.2).	connections for EACMS or SCI supporting EACMS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for PACS but~~ did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS or SCI supporting EACMS (Part 3.2).	required by Parts 3.1 and 3.2 (Requirement R3).

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 20~~19-03~~16-02
- CIP-005-8~~7~~ Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	TBD	Modified to address directives in FERC Order No. 850	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 33, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 **Balancing Authority**

4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 **Generator Operator**

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific Requirement Part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations]*.

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium impact BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.
1.2	Medium impact BCS with ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access, per system capability.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.4	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Monitor for unauthorized access through a physical access point into a PSP.	Examples of evidence may include, but are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a PSP.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a PSP and additional evidence that the alarm or alert was issued and communicated as identified in the Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Monitor each PACS for unauthorized physical access to a PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.
1.7	PACS associated with: • High impact BES Cyber Systems, or • Medium impact BES Cyber Systems with External Routable Connectivity SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each PSP, with information to identify the individual and date and time of entry.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes logging and recording of physical entry into each PSP and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each PSP that show the individual and the date and time of entry into each PSP.
1.9	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days.	Examples of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP that show the date and time of entry into each PSP.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each PSP.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require manual or automated logging of visitor entry into and exit from each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain visitor logs for at least 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	PACS associated with: - High impact BCS, or - Medium impact BCS with ERC Locally mounted hardware or devices at the PSP associated with: - High impact BCS, or - Medium impact BCS with ERC	Maintenance and testing of each PACS and locally mounted hardware or devices at each PSP at least once every 24 calendar months to ensure they function properly.	Examples of evidence may include, but are not limited to, a maintenance and testing program that provides for testing each PACS and locally mounted hardware or devices associated with each applicable each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. **Compliance Monitoring Process:**

   1.1. **Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

   1.2. **Evidence Retention:** The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
   - If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. **Compliance Monitoring and Assessment Processes:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				physical access point into a PSP. (Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each PACS for unauthorized physical access to a PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each PSP with sufficient information to identify the individual and date and time of

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least 90 days. (Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance	The Responsible Entity has documented and implemented a maintenance	The Responsible Entity has documented and implemented a maintenance	The Responsible Entity did not document or implement a maintenance and testing program

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Part 3.1)	and testing program for Physical Access Control Systems and locally mounted hardware or devices at the PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	and testing program for PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Part 3.1)	for PACS and locally mounted hardware or devices at the PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for PACS and locally mounted hardware or devices at the PSP, but did not complete required testing within 27 calendar months. (Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~third~~ fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
~~45~~53-day formal comment period with ballot	February 18 – April ~~4~~12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	~~April~~ October 2022
Board adoption	~~May~~ November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft ~~3~~ 4 Definitions"

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 **Balancing Authority**

4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 **Generator Operator**

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific Requirement Part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium impact BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.
1.2	Medium impact BCS with ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into ~~Physical Security Perimeters~~PSPs to only those individuals who have authorized unescorted physical access, per system capability.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.4	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Monitor for unauthorized access through a physical access point into a PSP.	Examples of evidence may include, but are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a PSP.

CIP-006-7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.5	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a PSP and additional evidence that the alarm or alert was issued and communicated as identified in the Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: - High impact BCS, or - Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Monitor each PACS for unauthorized physical access to a PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.
1.7	PACS associated with: - High impact BES Cyber Systems, or - Medium impact BES Cyber Systems with External Routable Connectivity SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each PSP, with information to identify the individual and date and time of entry.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes logging and recording of physical entry into each PSP and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each PSP that show the individual and the date and time of entry into each PSP.
1.9	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days.	Examples of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP that show the date and time of entry into each PSP.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R2 – Visitor Control Program			
Part	Applicable Systems	Requirements	Measures
2.1	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each PSP.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require manual or automated logging of visitor entry into and exit from each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor~~, except during CIP Exceptional Circumstances~~.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain visitor logs for at least 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	PACS associated with: - High impact BCS, or - Medium impact BCS with ERC Locally mounted hardware or devices at the PSP associated with: - High impact BCS, or - Medium impact BCS with ERC	Maintenance and testing of each PACS and locally mounted hardware or devices at each PSP at least once every 24 calendar months to ensure they function properly.	Examples of evidence may include, but are not limited to, a maintenance and testing program that provides for testing each PACS and locally mounted hardware or devices associated with each applicable each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				physical access point into a PSP. (Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each PACS for unauthorized physical access to a PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each PSP with sufficient information to identify the individual and date and time of

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9)
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least 90 days. (Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance	The Responsible Entity has documented and implemented a maintenance	The Responsible Entity has documented and implemented a maintenance	The Responsible Entity did not document or implement a maintenance and testing program

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Part 3.1)	and testing program for Physical Access Control Systems and locally mounted hardware or devices at the PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	and testing program for PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Part 3.1)	for PACS and locally mounted hardware or devices at the PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for PACS and locally mounted hardware or devices at the PSP, but did not complete required testing within 27 calendar months. (Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~third~~fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7~~6~~

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-7~~6~~:

4.2.3.1 Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5.1~~ identification and categorization processes.

4.3. **"Applicable Systems":** Each table has an "Applicable Systems" column to define the scope of systems to which a specific Requirement Part applies.

5. Effective Dates:

See "Project 2016-02 Modifications to CIP Standards Implementation Plan" ~~for CIP-006-6~~.

~~**6. Background:**~~

~~Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**“Applicable Systems” Columns in Tables:**~~

~~Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.~~

~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber~~

~~System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Locally mounted hardware or devices at the Physical Security Perimeter** – Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7~~6~~ Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations]*.

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7~~6~~ Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.1	Medium ~~I~~impact ~~BES Cyber Systems~~BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High ~~I~~impact BCS~~BES Cyber Systems~~, or • Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation that operational or procedural controls exist.

CIP-006-7~~6~~ Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable ~~Physical Security Perimeter~~PSP to only those individuals who have authorized unescorted physical access.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, language in the physical security plan that describes each ~~Physical Security Perimeter~~PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-6 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	~~Where technically feasible, u~~Utilize two or more different physical access controls (this does not require two completely independent ~~physical access control systems~~PACS) to collectively allow unescorted physical access into ~~Physical Security Perimeters~~PSPs to only those individuals who have authorized unescorted physical access, per system capability.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, language in the physical security plan that describes ~~the~~ each PSP~~Physical Security Perimeters~~ and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP.

CIP-006-7~~6~~ Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP to the personnel identified in the ~~BES~~ Cyber Security Incident response plan within 15 minutes of detection.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a ~~Physical Security Perimeter~~PSP and additional evidence that the alarm or alert was issued and communicated as identified in the ~~BES~~ Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High ~~I~~impact ~~BES Cyber Systems~~BCS, or • Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC SCI supporting an Applicable System in this Part	Monitor each ~~Physical Access Control System~~PACS for unauthorized physical access to a ~~Physical Access Control System~~PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-7~~6~~ Table R1– Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.7	~~Physical Access Control Systems (~~PACS~~)~~ associated with: • High ~~I~~impact BES Cyber Systems, or • Medium ~~I~~impact BES Cyber Systems with External Routable Connectivity SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized physical access to a ~~Physical Access Control System~~PACS to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to ~~Physical Access Control Systems~~PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the ~~BES~~ Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-7~~6~~ Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.8	High i~~I~~mpact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each ~~Physical Security Perimeter~~PSP, with information to identify the individual and date and time of entry.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in the physical security plan that describes logging and recording of physical entry into each ~~Physical Security Perimeter~~PSP and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into ~~Physical Security Perimeters~~each PSP that show the individual and the date and time of entry into ~~Physical Security Perimeter~~each PSP.

CIP-006-7~~6~~ Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each ~~Physical Security Perimeter~~PSP for at least ~~ninety~~ 90 calendar days.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, dated documentation such as logs of physical access into each ~~Physical Security Perimeters~~PSP that show the date and time of entry into each ~~Physical Security Perimeter~~PSP.

~~CIP-006-6 Table R1 — Physical Security Plan~~

~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~1.10~~	~~High Impact BES Cyber Systems and their associated:~~ ~~PCA~~ ~~Medium Impact BES Cyber Systems at Control Centers and their associated:~~ ~~PCA~~	~~Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.~~ ~~Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:~~ - ~~encryption of data that transits such cabling and components; or~~ - ~~monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or~~ - ~~an equally effective logical protection.~~	~~An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.~~

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7~~6~~ Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each ~~Physical Security Perimeter~~PSP~~, except during CIP Exceptional Circumstances~~.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, language in a visitor control program that requires continuous escorted access of visitors within each ~~Physical Security Perimeters~~PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-7~~6~~ Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require manual or automated logging of visitor entry into and exit from ~~the Physical Security Perimeter~~each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor~~, except during CIP Exceptional Circumstances~~.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, language in a visitor control program that requires continuous escorted access of visitors within ~~Physical Security Perimeters~~each PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7~~6~~ Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain visitor logs for at least ~~ninety~~ 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ~~ninety~~ 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7~~6~~ Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7~~6~~ Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	~~Physical Access Control Systems (~~PACS~~)~~ associated with: • High ~~I~~impact ~~BES Cyber Systems~~BCS, or • Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC Locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP associated with: • High ~~I~~impact ~~BES Cyber Systems~~BCS, or • Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC	Maintenance and testing of each ~~Physical Access Control System~~PACS and locally mounted hardware or devices at ~~the Physical Security Perimeter~~each PSP at least once every 24 calendar months to ensure they function properly.	~~An e~~Examples of evidence may include, but ~~is~~are not limited to, a maintenance and testing program that provides for testing each ~~Physical Access Control System~~PACS and locally mounted hardware or devices associated with each applicable ~~Physical Security Perimeter~~each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~1.4. Additional Compliance Information:~~

~~None~~

~~2. Table of Compliance Elements~~Violation Security Levels

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Part 1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP. (Part 1.4)

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-006-7~~6~~)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td></td><td>OR
The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~ PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5)
OR
The Responsible Entity does not have a process to monitor each ~~Physical Access Control System~~PACS for unauthorized physical access to a ~~Physical Access Control Systems~~PACS. (Part 1.6)
OR
The Responsible Entity does not have a process to alert for unauthorized physical access to ~~Physical Access Control Systems~~PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7)
OR
The Responsible Entity does not have a process to log authorized physical entry into each ~~Physical Security Perimeter~~PSP with sufficient information to identify the individual and date and time of entry. (Part</td></tr>
</table>

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9) ~~OR~~ ~~The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)~~
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ~~ninety~~ 90 days. (Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months.	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for ~~Physical Access Control Systems~~ PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required testing within 27 calendar months. (Part 3.1)

R #	Violation Severity Levels (CIP-006-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	(Part 3.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of	

Version	Date	Action	Change Tracking
		Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~General:~~

~~While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.~~

~~Requirement R1:~~

~~Methods of physical access control include:~~

- ~~Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~
- ~~Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~
- ~~Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~

- ~~Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.~~

~~Methods to monitor physical access include:~~

- ~~Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.~~
- ~~Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.~~

~~Methods to log physical access include:~~

- ~~Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.~~
- ~~Video Recording: Electronic capture of video images of sufficient quality to determine identity.~~
- ~~Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.~~

~~The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.~~

~~Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.~~

~~The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the~~

~~physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.~~

~~This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.~~

~~The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.~~

~~The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an "an equally effective logical protection" in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.~~

~~The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity's BES Cyber Systems while not requiring controls to be~~

~~implemented on third-party components when entities rely on leased third-party communications.~~

~~In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.~~

~~Requirement R2:~~

~~The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.~~

~~The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.~~

~~Requirement R3:~~

~~This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.~~

~~Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable~~

~~communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.~~

~~Rationale for Requirement R2:~~

~~To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.~~

~~Rationale for Requirement R3:~~

~~To ensure all Physical Access Control Systems and devices continue to function properly.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 4 Definitions”.

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002- identification and categorization processes.

4.3. “Applicable Systems”: Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See Project 2016-02 Modifications to CIP Standards Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1– System Hardening			
Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports or network accessible logical services, individually or by group. • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; or • Configuration or settings of host-based firewalls or other device level mechanisms that disable or prevent unneeded network accessible logical ports or network accessible logical services.

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium impact BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Examples of evidence may include, but are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting: High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources, excluding storage resources, between Virtal Cyber Assets (VCAs) that are not of, or associated with, the same impact categorization.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.	Examples of evidence may include, but are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.
2.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Examples of evidence may include, but are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	this Part		
2.3	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.
2.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Examples of evidence may include, but are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of evidence may include, but are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
	this Part		
3.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Examples of evidence may include, but are not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events (per system capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use.
5.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Identify individuals who have authorized access to shared accounts.	Examples of evidence may include, but are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information:

None

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)	The Responsible Entity had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization. (Part 1.3)	The Responsible Entity neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days	The Responsible Entity did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2)	The Responsible Entity did not include any processes for installing cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R2. (Requirement R2) OR The Responsible Entity did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity did not obtain approval by the CIP

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-007-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>but less than 50 calendar days of the evaluation completion. (Part 2.3)</td><td>OR
The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)</td><td>security patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)</td><td>Senior Manager or delegate. (Part 2.4)
OR
The Responsible Entity did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)</td></tr>
<tr><td>R3</td><td>N/A</td><td>The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)</td><td>The Responsible Entity did not mitigate the threat of detected malicious code. (Part 3.2)
OR
The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).</td><td>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3).
OR
The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)</td></tr>
<tr><td>R4</td><td>The Responsible Entity missed one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)</td><td>The Responsible Entity missed one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)</td><td>The Responsible Entity did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2)
OR
The Responsible Entity did not retain applicable security</td><td>The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4)
OR
The Responsible Entity, per system capability, did not detect</td></tr>
</table>

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity missed two or more 15 calendar day intervals. (Part 4.4)	and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)
R5	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity did not, per device capability, change known default passwords. (Part 5.4) OR

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity process(es) for password-only authentication for interactive user access did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity neither limited the number of unsuccessful authentication attempts nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining

Version	Date	Action	Change Tracking
			directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~second~~ fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
~~45~~53-day formal comment period with ballot	February 18 – April ~~4~~12, 2022
45-day formal comment period with ballot	August 10 – September 30, 2022

Anticipated Actions	Date
Final Ballot	~~April~~October 2022
Board adoption	~~May~~ November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See ~~S~~separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 4~~3~~ Definitions".

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems~~,~~ associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002- identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See Project 2016-02 Modifications to CIP Standards Implementation Plan ~~for CIP-007-7~~.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1– System Hardening

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports ~~and~~ or network accessible logical services, individually or by group. • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; or • Configuration or settings of host-based firewalls or other device level mechanisms that disable~~s~~ or prevent~~s~~ unneeded network accessible logical ports or network accessible logical services.

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium impact BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Examples of evidence may include, but are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting: High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources, excluding storage resources, between Virtual Cyber Assets (VCAs) that are not of, or associated with, the same impact categorization.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as:~~.~~ • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.	Examples of evidence may include, but are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.

CIP-007-7 Table R2 – Security Patch Management			
Part	Applicable Systems	Requirements	Measures
2.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Examples of evidence may include, but are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.

CIP-007-7 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Examples of evidence may include, but are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of evidence may include, but are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part		
3.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Examples of evidence may include, but are not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the ~~BCS~~ Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events (per ~~Cyber Asset or BCS~~system capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
	this Part		
4.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use.
5.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Identify individuals who have authorized access to shared accounts.	Examples of evidence may include, but are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: - Records of a procedure that passwords are changed when new devices are in production; or - Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: - System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or - Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: - System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or - Attestations that include a reference to the documented procedures that were followed.
5.7	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: - Documentation of the account-lockout parameters; or - Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information:

None

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)	The Responsible Entity had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization. (Part 1.3)	The Responsible Entity neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days	The Responsible Entity did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2)	The Responsible Entity did not include any processes for installing cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R2. (Requirement R2) OR The Responsible Entity did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity did not obtain approval by the CIP

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	but less than 50 calendar days of the evaluation completion. (Part 2.3)	OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	security patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)	Senior Manager or delegate. (Part 2.4) OR The Responsible Entity did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)
R3	N/A	The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3). OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity missed one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	The Responsible Entity missed one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity did not retain applicable security	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity, per system capability, did not detect

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity missed two or more 15 calendar day intervals. (Part 4.4)	and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)
R5	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity did not, per device capability, change known default passwords. (Part 5.4) OR

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity process(es) for password-only authentication for interactive user access did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity neither limited the number of unsuccessful authentication attempts nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining

Version	Date	Action	Change Tracking
			directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 10 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 4 Definitions”

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7~~6~~

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~4.1.6~~4.1.5 **Reliability Coordinator**

~~4.1.7~~4.1.6 **Transmission Operator**

~~4.1.8~~4.1.7 **Transmission Owner**

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**:

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-007-7~~6~~:

4.2.3.1 Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-~~5.1~~7 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates:

See Project 2016-02 Modifications to CIP Standards Implementation Plan ~~for CIP-007-7"~~6.

~~**6. Background:**~~

~~Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a~~

~~program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~“Applicable Systems” Columns in Tables:~~

~~Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~

~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R1 – ~~Ports and Services~~System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R1 –~~ Ports and Services~~System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. ~~Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.~~	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports or network accessible logical services~~on all applicable Cyber Assets and Electronic Access Points~~, individually or by group. • Listings of the listening ports~~on the Cyber Assets~~, individually or by group, from either ~~the device~~ configuration files or settings, command output (such as netstat), or network scans of open ports; or • Configuration or settings ~~files~~ of host-based firewalls or other device level mechanisms that disable or prevent unneeded network accessible logical ~~only allow needed~~ ports or network accessible logical services~~and deny all others~~.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

CIP-007-7~~6~~ Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting: High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources, excluding storage resources, between Virtual Cyber Assets (VCAs) that are not of, or associated with, the same impact categorization.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared~~.~~, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	A patch management process for tracking, evaluating, and installing cyber security patches ~~for applicable Cyber Assets~~. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for ~~applicable Cyber Assets~~Applicable Systems that are updateable and for which a patching source exists.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored~~, whether on an individual BES Cyber System or Cyber Asset basis~~.

CIP-007-7~~6~~ Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security~~-related~~ patches released by the documented sources at least once every 35 calendar days.

CIP-007-7~~6~~ Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.3	High ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; or - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: - Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of ~~BES Cyber System C~~component software revision, or registry exports that show software has been installed); or - A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.

CIP-007-7~~6~~ Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Deploy method(s) to deter, detect, or prevent malicious code.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-7~~6~~ Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: - Records of response processes for malicious code detection - Records of the performance of these processes when malicious code is detected.
3.3	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Log security events, per system capability, ~~at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)~~ for identification of, ~~and after-the-fact investigations of,~~ Cyber Security Incidents that include~~s~~, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the ~~BES Cyber System~~~~BCS~~Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-7~~6~~ Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Generate alerts for security events that the Responsible Entity determines necessitates an alert~~,~~ that includes, as a minimum, each of the following types of events (per Cyber Asset or ~~BES Cyber System~~BCS capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7~~6~~ Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Where technically feasible, r~~Retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, ~~any~~ findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7~~6~~ Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Have a method(s) to enforce authentication of interactive user access, ~~where technically feasible~~per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use ~~for the BES Cyber System~~.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Identify individuals who have authorized access to shared accounts.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Change known default passwords, per ~~Cyber Asset~~system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-7~~6~~ Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.5	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the ~~Cyber Asset~~Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the ~~Cyber Asset~~Applicable System.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7~~6~~ Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Where technically feasible, f~~For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7~~6~~ Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.7	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Where technically feasible, either:~~ Limit the number of unsuccessful authentication attempts~~;~~ or ~~G~~generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1) ~~N/A~~	The Responsible Entity ~~has implemented and documented processes for Ports and Services but~~ had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity ~~has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,~~ had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are not of, or associated with, the same impact categorization. (Part 1.3)	The Responsible Entity ~~did not~~ neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity ~~has documented and implemented one or~~	The Responsible Entity ~~has documented or implemented one or more~~	The Responsible Entity ~~has documented or implemented one or more~~	The Responsible Entity did not implement or document one or more process(es) that included the

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	~~more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan,	~~process(es) for patch management but~~ did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for ~~a~~Applicable Systems ~~Cyber Assets~~. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR	~~process(es) for patch management but~~ did not include any processes for installing cyber security patches for ~~a~~Applicable Systems ~~Cyber Assets~~. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but,~~	applicable items in CIP-007-7~~6~~ Table R2. (Requirement R2) OR The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but~~ did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch but~~ did not implement the plan as

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	~~in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)	created or revised within the timeframe specified in the plan. (Part 2.4)
R3	N/A	The Responsible Entity ~~has implemented one or more documented process(es), but~~, where signatures or patterns are used, the Responsible Entity did not address testing the	The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not mitigate the threat of detected malicious code. (Part 3.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3). OR

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		signatures or patterns. (Part 3.3)	The Responsible Entity, ~~has implemented one or more documented process(es) for malicious code prevention, but~~ where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but~~ missed one of 15 calendar day ~~an~~ interval and completed the review within 22	The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but~~ missed ~~an~~ one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity ~~has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but~~ did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity ~~has documented and~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity, per system capability, ~~has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but~~ did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar days of the prior review. (Part 4.4)		~~implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but~~ did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity ~~has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but~~ missed two or more 15 calendar day intervals. (Part 4.4)	

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification or inventory of -all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity ~~has implemented one or more documented process(es) for~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~password-only authentication for interactive user access that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented~~ process(es) for password-only authentication for interactive user access ~~that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for~~	The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but~~ did not, per device capability, change known default passwords. (Part 5.4) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity~~ did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation

R #	Violation Severity Levels (CIP-007-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	to change the password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either~~neither limited the number of unsuccessful authentication attempts nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.~~

~~**1.1.** This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'~~

~~1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.~~

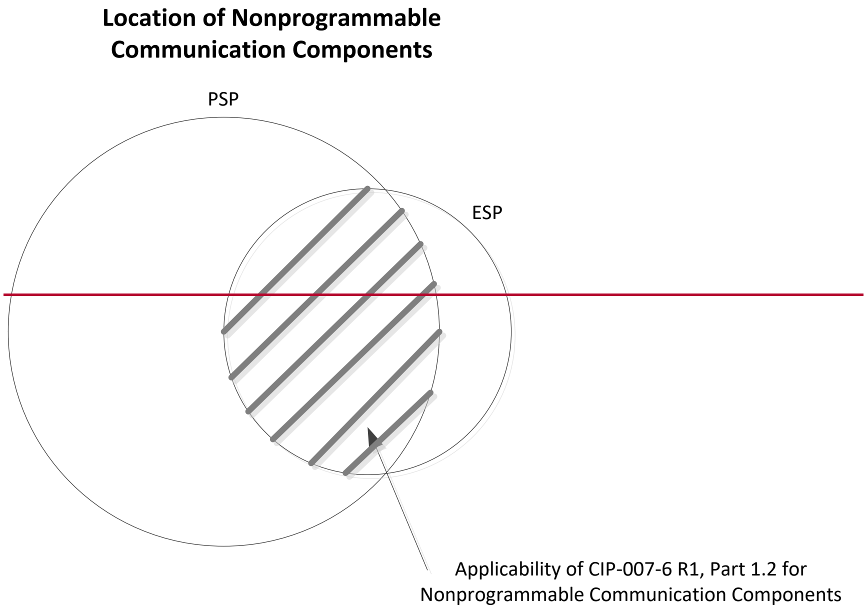
~~The protection of these ports can be accomplished in several ways including, but not limited to:~~

- ~~Disabling all unneeded physical ports within the Cyber Asset's configuration~~
- ~~Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization~~
- ~~Physical port obstruction through removable locks~~

~~The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.~~

~~This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.~~

~~The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:~~



~~**Requirement R2:**~~

~~The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.~~

~~Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.~~

~~One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.~~

~~**2.1.** The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they~~

~~can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.~~

~~**2.2.** Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.~~

~~When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.~~

~~**2.3.** The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or~~

~~those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.~~

~~**2.4.** The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.~~

~~**Requirement R3:**~~

~~**3.1.** Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.~~

~~**3.2.** When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or~~

~~method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.~~

~~Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media (“transient devices”) in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.~~

~~**3.3.** In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System’s ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a ‘false positive’ could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.~~

~~**Requirement R4:**~~

~~Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.~~

~~**4.1.** In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.~~

~~Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.~~

~~User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.~~

~~It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.~~

~~**4.2.** Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.~~

~~The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:~~

- ~~Detected known or potential malware or malicious activity~~
- ~~Failure of security event logging mechanisms~~
- ~~Login failures for critical accounts~~
- ~~Interactive login of system accounts~~
- ~~Enabling of accounts~~
- ~~Newly provisioned accounts~~
- ~~System administration or change tasks by an unauthorized user~~
- ~~Authentication attempts on certain accounts during non-business hours~~
- ~~Unauthorized configuration changes~~
- ~~Insertion of Removable Media in violation of a policy~~

~~**4.3** Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.~~

~~**4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-~~

~~time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.~~

~~**Requirement R5:**~~

~~Account types referenced in this guidance typically include:~~

- ~~Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.~~
- ~~Individual user account: An account used by a single user.~~
- ~~Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.~~
- ~~System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.~~
- ~~Application account: A specific system account, with rights granted at the application level often used for access into a Database.~~
- ~~Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.~~
- ~~Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.~~
- ~~Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.~~

~~**5.1** Reference the Requirement's rationale.~~

~~**5.2** Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.~~

~~**5.3** Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.~~

~~**5.4.** Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.~~

~~The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.~~

~~**5.5.** Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.~~

~~Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.~~

~~**5.6** Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.~~

~~**5.7** Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.~~

~~Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.~~

~~In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.~~

~~The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).~~

~~Rationale for Requirement R2:~~

~~Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.~~

~~Rationale for Requirement R3:~~

~~Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.~~

~~Rationale for Requirement R4:~~

~~Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.~~

~~Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.~~

~~Rationale for Requirement R5:~~

~~To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.~~

~~Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.~~

~~Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.~~

~~Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.~~

~~For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.~~

~~The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.~~

~~The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.~~

~~The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.~~

~~Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 4 Definitions".

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the Bulk Electric System (BES):

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BES) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*.

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated Electronic Access Control and Monitoring Systems (EACMS) Medium impact BCS and their associated EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the Applicable Systems column for this Part; and	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column including justification for attempt determination criteria and documented processes for notification.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
		1.2.3 To provide notification per Requirement R4.	
1.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the Applicable Systems column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	Examples of evidence may include, but are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	Examples of evidence may include, but are not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column according to the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and CISA, or their successors.
4.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and CISA, or their successors.

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
		the Applicable Systems column for this Part.	
4.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and CISA, or their successors.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible Entity's plan did not include one or more processes to provide notification per Requirement R4. (Part 1.2) OR The Responsible Entity's plan did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	The Responsible Entity did not develop a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible Entity's plan did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the Applicable Systems column for Part 1.2. (Part 1.2)
R2	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 18 calendar months

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-008-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>months between tests of the plan(s). (Par 2.1)</td><td>months between tests of the plan(s). (Part 2.1)</td><td>months between tests of the plan(s). (Part 2.1)
OR
The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column for Part 2.2 occurs. (Part 2.2)</td><td>between tests of the plan(s). (Part 2.1)
OR
The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the Applicable Systems column for Part 2.3. (Part 2.3)</td></tr>
<tr><td>**R3**</td><td>The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)</td><td>The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2)
OR
The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120</td><td>The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)
OR
The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a</td><td>The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)</td></tr>
</table>

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR The Responsible Entity did not update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	
R4	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not report on one or more of the	The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not notify E-ISAC or CISA, or their	The Responsible Entity did not notify E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3) OR The Responsible Entity did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)	Applicable Systems column. (Requirement R4)	successors, of a Reportable Cyber Security Incident. (Requirement R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~third~~ fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
~~45~~53-day formal comment period with ballot	February 18 – April ~~4~~12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	~~April~~ October 2022
Board adoption	~~May~~ November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 4~~3~~ Definitions".

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 **Balancing Authority**

4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the Bulk Electric System (BES):

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 **Generator Operator**

4.1.4 **Generator Owner**

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BES) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*.

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated Electronic Access Control and Monitoring Systems (EACMS) Medium impact BCS and their associated EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the Applicable Systems column for this Part; and	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column including justification for attempt determination criteria and documented processes for notification.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
		1.2.3 To provide notification per Requirement R4.	
1.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the Applicable Systems column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	Examples of evidence may include, but are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

M4.

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of -post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	Examples of evidence may include, but are not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column according to the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and CISA, or their successors.
4.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and CISA, or their successors.

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	Applicable Systems	Requirements	Measures
		the Applicable Systems column for this Part.	
4.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and CISA, or their successors.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible Entity's plan did not include one or more processes to provide notification per Requirement R4. (Part 1.2) OR The Responsible Entity's plan did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	The Responsible Entity did not develop a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible Entity's plan did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the Applicable Systems column for Part 1.2. (Part 1.2)
R2	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 18 calendar months

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months between tests of the plan(s). (Par 2.1)	months between tests of the plan(s). (Part 2.1)	months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column for Part 2.2 occurs. (Part 2.2)	between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the Applicable Systems column for Part 2.3. (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1) OR The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR The Responsible Entity did not update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	
R4	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not report on one or more of the	The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not notify E-ISAC or CISA, or their	The Responsible Entity did not notify E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3) OR The Responsible Entity did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)	Applicable Systems column. (Requirement R4)	successors, of a Reportable Cyber Security Incident. (Requirement R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 4 Definitions”

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7~~6~~

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the Bulk Electric System (BES):

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Remedial Action Scheme~~RAS where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-7~~6~~:

4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BES) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates:

See "Project 2016-02 Modifications to CIP Standards Implementation Plan" ~~for CIP-008-6~~.

~~**6. Background:**~~

~~Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~6~~7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*.

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~6~~ 7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~Electronic Access Control and Monitoring Systems (EACMS) Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: - A Reportable Cyber Security Incident; or - An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the ~~“~~Applicable Systems~~”~~ column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column including justification for attempt determination criteria and documented processes for notification.
1.3	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~EACMS Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

CIP-008-7~~6~~ Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated~~:~~ EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. -Types of exercises may include discussion or operations based exercises.

CIP-008-7~~6~~ Table R2 – Cyber Security Incident Response Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the ~~“~~"Applicable Systems~~”~~" column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.
2.3	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~ EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the ~~“~~"Applicable Systems~~”~~" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the ~~“~~"Applicable Systems~~”~~" column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, all of the following: 1. Dated documentation of- post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-7~~6~~ Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated ~~:~~EACMS Medium ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated ~~:~~EACMS SCI supporting an Applicable System in this Part	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA)~~National Cybersecurity and Communications Integration Center (NCCIC)~~, ~~[1]~~ or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the ~~“~~Applicable Systems~~”~~ column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column according to the applicable requirement parts in *CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~EACMS Medium ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated ~~:~~EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and ~~NCCIC~~CISA, or their successors.

~~[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).~~

CIP-008-7~~6~~ Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
4.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~EACMS SCI supporting an Applicable System in this Part	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ~~NCCIC~~CISA, or their successors.
4.3	High ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated ~~:~~EACMS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated ~~:~~EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within ~~7~~ seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and ~~NCCIC~~CISA, or their successors.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:
The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:
The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~
- ~~Complaint~~

~~**1.4. Additional Compliance Information:**~~
~~None~~

2. Table of Compliance Elements

R #	Violation Severity Levels (CIP-008-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~ did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible Entity's ~~has developed a Cyber Security Incident response plan, but the~~ plan ~~does~~ did not include one or more processes to	The Responsible Entity ~~has~~ did not develop~~ed~~ a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible Entity's ~~has developed a Cyber Security Incident response plan, but the~~ plan ~~does~~did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the ~~"~~Applicable Systems~~"~~ column for Part 1.2. (Part 1.2)

			provide notification per Requirement R4. (Part 1.2) OR The Responsible Entity's ~~has developed a Cyber Security Incident response plan, but the~~ plan ~~does~~ did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	
R2	The Responsible Entity ~~has~~ did not test~~ed~~ the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Par 2.1)	The Responsible Entity ~~has~~did not test~~ed~~ the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity ~~has~~ did not test~~ed~~ the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.2 occurs. (Part 2.2)	The Responsible Entity ~~has~~ did not test~~ed~~ the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.3. (Part 2.3)

R3	The Responsible Entity ~~has~~did not notify~~ied~~ each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	The Responsible Entity ~~has~~did not update~~d~~ the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity ~~has~~ did not notify~~ied~~ each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1) OR The Responsible Entity ~~has~~ did not update~~d~~ the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity ~~has~~ did not update~~d~~ the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)

		The Responsible Entity ~~has~~ did not update~~d~~ the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	
R4	The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.2 but failed~~ did not ~~to~~ notify	The Responsible Entity ~~failed to~~did not notify E-ISAC or ~~NCCIC~~CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system	The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to~~did not notify or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2)	The Responsible Entity ~~failed to~~did not notify E-ISAC and ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

	or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.3 but failed to~~did not report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3) OR The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber~~	identified in the ~~“~~Applicable Systems~~”~~ column. (Requirement R4)	OR The Responsible Entity ~~failed to~~did not notify E-ISAC or ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	

	~~Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the "Applicable Systems" column for Part 4.1 but failed to~~ did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed

Version	Date	Action	Change Tracking
			from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 4 Definitions".

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*.

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	Examples of evidence may include, but are not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover Applicable System functionality.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Examples of evidence may include, but are not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Examples of evidence may include, but are not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	Examples of evidence may include, but are not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover Applicable System functionality substitutes for this test.	Examples of evidence may include, but are not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
		An actual recovery response may substitute for an operational exercise.	• An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable Requirement Parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the Applicable Requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated:	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:	Examples of evidence may include, but are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS	3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:
As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:
The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information: None

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity's plan(s) did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity plan(s) did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity did not create recovery plan(s) for Applicable Systems. OR The Responsible Entity plan(s) did not address the conditions for activation in Part 1.1. OR The Responsible Entity plan(s) did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to	The Responsible Entity did not test the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 16 calendar months, not exceeding 17	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 17 calendar	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 18 calendar months between tests. (Part 2.2) OR

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)	calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)	months, not exceeding 18 calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)	The Responsible Entity did not test the recovery plan(s) according to Part 2.3 within 39 calendar months between tests of the plan(s). (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Part 3.1.3)	The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3)	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1) OR The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2)	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		OR The Responsible Entity did not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part 3.2)	OR The Responsible Entity did not update the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~second~~ fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
~~45~~53-day formal comment period with ballot	February 18 – April ~~4~~12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	~~April~~ October 2022
Board adoption	~~May~~November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 4~~3~~ Definitions".

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*.

CIP-009-7 Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	Examples of evidence may include, but are not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover Applicable System functionality.

CIP-009-7 Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Examples of evidence may include, but are not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Examples of evidence may include, but are not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: - By recovering from an actual incident; - With a paper drill or tabletop exercise; or - With an operational exercise.	Examples of evidence may include, but are not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover Applicable System functionality substitutes for this test.	Examples of evidence may include, but are not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.	Examples of evidence may include, but are not limited to, dated documentation of: - An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
		An actual recovery response may substitute for an operational exercise.	- An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable Requirement Parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the Applicable Requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated:	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:	Examples of evidence may include, but are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS	3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information: None

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	N/A	The Responsible Entity's plan(s) did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity plan(s) did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity did not create recovery plan(s) for Applicable Systems. OR The Responsible Entity plan(s) did not address the conditions for activation in Part 1.1. OR The Responsible Entity plan(s) did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to	The Responsible Entity did not test the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 16 calendar months, not exceeding 17	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 17 calendar	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 18 calendar months between tests. (Part 2.2) OR

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)	calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)	months, not exceeding 18 calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)	The Responsible Entity did not test the recovery plan(s) according to Part 2.3 within 39 calendar months between tests of the plan(s). (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Part 3.1.3)	The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3)	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1) OR The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2)	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1)

R #	**Violation Severity Levels (CIP-009-7)**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
		OR The Responsible Entity did not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part 3.2)	OR The Responsible Entity did not update the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
45-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7~~6~~

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~**Interchange Coordinator or Interchange Authority**~~

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Special Protection System or Remedial Action Scheme~~RAS where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-7~~6~~:

4.2.3.1 Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2~~**4.2.3.3** Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **"Applicable Systems":** Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan"~~ for CIP-009-6~~.

~~6. Background:~~

~~Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~“Applicable Systems” Columns in Tables:~~

~~Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.~~

~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable ~~r~~Requirement ~~p~~Parts in *CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable ~~r~~Requirement ~~p~~Parts in *CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications*.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover ~~BES Cyber~~ Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover ~~BES Cyber~~Applicable System functionality.

CIP-009-7~~6~~ Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.4	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per ~~Cyber Asset~~system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable ~~r~~Requirement ~~p~~Parts in *CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable ~~r~~Requirement ~~p~~Parts in *CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: - By recovering from an actual incident; - With a paper drill or tabletop exercise; or - With an operational exercise.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-7~~6~~ Table R2 – Recovery Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover ~~BES Cyber~~ Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover ~~BES Cyber~~Applicable System functionality substitutes for this test.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High ~~I~~impact BCS~~BES Cyber Systems~~	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable ~~r~~Requirement ~~p~~Parts in *CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the ~~a~~Applicable ~~r~~Requirement parts in *CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication			
Part	Applicable Systems	Requirements	Measures
3.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS ~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	~~An e~~Examples of evidence may include, but are~~is~~ not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-7~~6~~ Table R3 – Recovery Plan Review, Update and Communication

Part	Applicable Systems	Requirements	Measures
3.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact ~~-~~the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity's ~~has developed recovery plan(s), but the~~ plan(s) ~~do~~ did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity ~~has developed recovery plan(s), but the~~ plan(s) ~~do~~ did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity ~~has~~ did not create~~d~~ recovery plan(s) for ~~BES Cyber~~Applicable Systems. OR The Responsible Entity ~~has created recovery plan(s) for BES Cyber Systems, but the~~ plan(s) ~~does~~ did not address the conditions for activation in Part 1.1. OR The Responsible Entity ~~has created recovery plan(s) for BES Cyber Systems, but the~~ plan(s) ~~does~~ did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan(s) according to ~~R2~~ Part 2.1 within 15 calendar months, not exceeding 16 calendar months	The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1)	The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan(s) according to ~~R2~~ Part 2.1 within 17 calendar months, not exceeding 18 calendar months between	The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan(s) according to ~~R2~~ Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	between tests of the plan(s). (Part 2.1) OR The Responsible Entity ~~has~~ did not test~~ed~~ a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not test~~ed~~ the recovery plan according to ~~R2~~ Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)	OR The Responsible Entity ~~has~~ did not test~~ed~~ a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan according to ~~R2~~ Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)	tests of the plan. (Part 2.1) OR The Responsible Entity ~~has~~ did not test~~ed~~ a representative sample of the information used in the recovery of ~~BES Cyber~~ Applicable System functionality according to ~~R2~~ Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan according to ~~R2~~ Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)	The Responsible Entity ~~has~~ did not test~~ed~~ a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 18 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~ did not test~~ed~~ the recovery plan(s) according to ~~R2~~ Part 2.3 within 39 calendar months between tests of the plan(s). (Part 2.3)
R3	The Responsible Entity ~~has~~ did not notify~~ied~~ each person or group	The Responsible Entity ~~has~~ did not update~~d~~ the recovery plan(s) based on	The Responsible Entity ~~has~~ neither documented lessons learned nor	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Part 3.1.3)	any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity ~~has~~ did not notify~~ied~~ each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3) OR The Responsible Entity ~~has~~ did not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact	documented the absence of any lessons learned within 90 and less than 120 calendar days -of each recovery plan test or actual recovery. (Part 3.1.1) OR The Responsible Entity ~~has~~ did not update~~d~~ the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity ~~has~~ did not update~~d~~ the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact	absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7~~6~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Responders, or • Technology changes. (Part 3.2)	the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	

Version	Date	Action	Change Tracking
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~The following guidelines are available to assist in addressing the required components of a recovery plan:~~

- ~~NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf~~
- ~~National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf~~

~~The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.~~

~~A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.~~

~~For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.~~

~~For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.~~

~~For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:~~

1. ~~Installation files and media;~~
2. ~~Current backup tapes and any additional documented configuration settings;~~
3. ~~Documented build or restoration procedures; and~~
4. ~~Cross site replication storage.~~

~~For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:~~

- ~~Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.~~
- ~~Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.~~
- ~~Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.~~
- ~~Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.~~

~~The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.~~

~~For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.~~

~~Requirement R2:~~

~~A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.~~

~~A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.~~

~~Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, “A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures.”~~

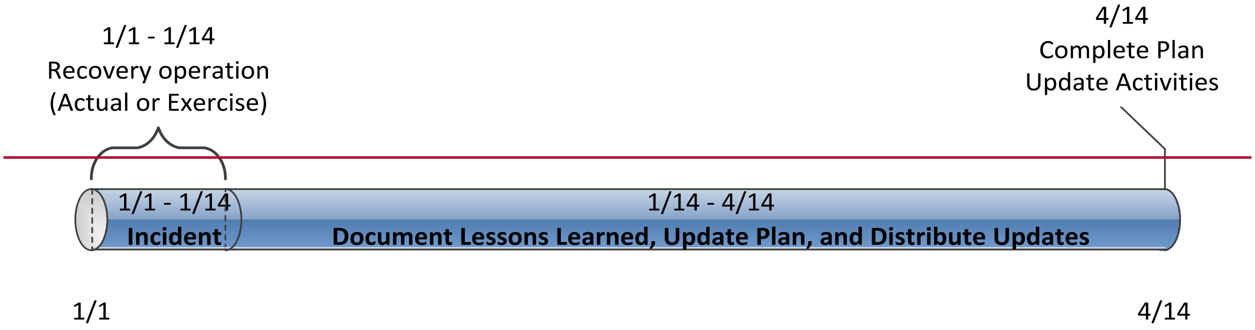
~~The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, “[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and ‘boots on the ground’ response (e.g., firefighters decontaminating mock victims).”~~

~~For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.~~

~~Requirement R3:~~

~~This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.~~

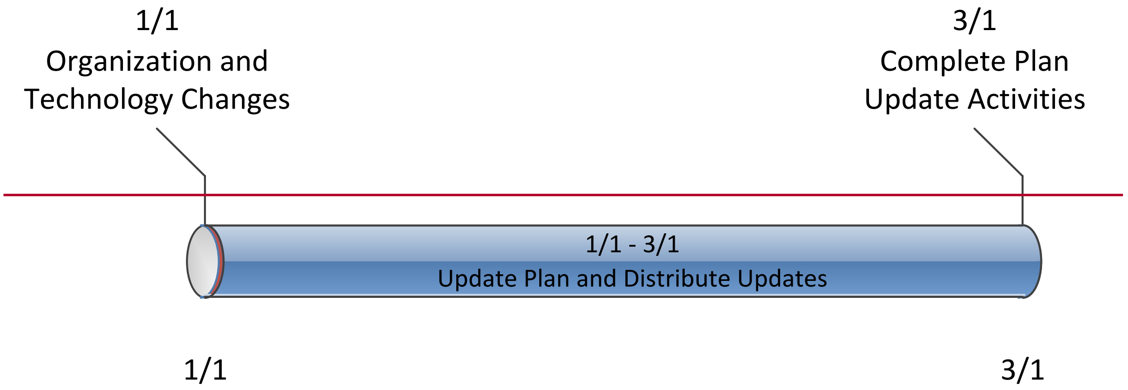
~~The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.~~



~~Figure 1: CIP-009-6 R3 Timeline~~

~~The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.~~

~~The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.~~



~~Figure 2: Timeline for Plan Changes in 3.2~~

~~When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.~~

~~Rationale for Requirement R2:~~

~~The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.~~

~~Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.~~

~~Rationale for Requirement R3:~~

~~To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed of modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **"Applicable Systems":** Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. **Effective Date:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manages changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Security Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Security Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Control the implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007. For those changes: 1.1.1. Authorize the changes; and 1.1.2. Verify the required cyber security controls remain implemented as required as a part of the change. Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.	Examples of evidence may include, but are not limited to, a documented process that controls intended changes to settings that may weaken cyber security controls in CIP-005 and CIP-007, such as: • Operating system (OS) software; • Firmware; • Commercially available or open-source application software, including application containers; • Custom software installed, including application containers; • Configuration that modifies network accessible logical ports or network accessible services on an Applicable System; • SCI configuration of host affinity control between systems with different impact ratings; • Changes to configurations or settings for an ESP between systems with different impact ratings;

CIP-010-5 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			- Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations; or - Any other configuration or setting determined by the Responsible Entity. (1.1.1.) - A change request record and associated authorization for applicable changes; or - Records from a change management system that identifies applicable changes and records of authorization for changes. (1.1.2.) - A list of cyber security controls verified along with the dated results; or - A dated output from cyber security tools such as a vulnerability scanner.
1.2	High impact BCS	1.2.1. Prior to implementing an intended change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 and	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

CIP-010-5 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		CIP-007 remain implemented as required; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Security Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Security Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Security Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Methods to monitor at least once every 35 calendar days for unauthorized changes to software, or unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007, per system capability. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs or records from a system that is monitoring for unauthorized changes along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.
3.2	High impact BES Cyber Systems SCI supporting an Applicable System in this Part	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
		performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: - Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System; or - CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: - The output of any tools used to perform the assessment, or - Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.
3.4	High impact BCS and their associated:	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of	Examples of evidence may include, but are not limited to: - Reports or logs from automated mechanisms that perform

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
	1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	completing the action plan and the execution status of any remediation or mitigation action items.	remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority:** "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.		The Responsible Entity's change management process(es) does not include two of the required items listed in 1.1.1 through 1.1.3. (Part 1.1); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity change management process(es) did not include the three required items listed in 1.1.1 through 1.1.3. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. (Part 1.2); OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity neither documented nor implemented any change management process(es) that include required items in Part 1.1 through Part 1.2. (Requirement R1)
R2.	N/A	N/A	The Responsible Entity did not document nor implemented a process(es) with methods to monitor for unauthorized changes at least once every 35 calendar days. (Part 2.1); OR	The Responsible Entity neither documented nor implemented a process(es) with methods to monitor for, i at least once every 35 calendar days and neither documented nor investigated detected

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1);	unauthorized changes. (Part 2.1)
R3.	The Responsible Entity performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity did not implement any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3) OR The Responsible Entity performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2) OR The Responsible Entity did not perform the active

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				vulnerability assessment of a Cyber System prior to it becoming an Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)
R4.	The Responsible Entity did not manage its Transient Cyber Asset(s) according to Attachment 1, Section 1.1. (Requirement R4) OR The Responsible Entity did not document the Removable Media sections according to	The Responsible Entity did not implement the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities,	The Responsible Entity did not authorize its TCA(s) according to Attachment 1, Section 1.2. (R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities, mitigation for the introduction	The Responsible Entity did not document or implement one or more plan(s) for TCAs and Removable Media according to Requirement R4. (Requirement R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document authorization for TCA managed by the Responsible Entity according to Attachment 1, Section 1.2. (Requirement R4)	mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCA managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4)	of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.
- CIP-010-5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. <u>TCA Management</u>: Responsible Entities shall manage TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. <u>TCA Authorization</u>: For each individual or group of TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. <u>Software Vulnerability Mitigation</u>: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. <u>Introduction of Malicious Code Mitigation</u>: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. <u>Unauthorized Use Mitigation</u>: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCA(s). This can be included as part of the TCA(s), part of the documentation related to authorization of TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, methods to maintain the known good state of the OS and all software, or system hardening practices. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, controls to maintain the known good state of the OS and all software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, controls to maintain the known good state of the OS and all software by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~third~~ fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53~~45~~-day formal comment period with ballot	February 18 – April 12~~4~~, 2022
45-day formal comment period with ballot	August 10 – September 30, 2022

Anticipated Actions	Date
Final Ballot	~~April~~October 2022
Board adoption	~~May~~November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled “Project 2016-02 Draft 4~~3~~ Definitions”.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manages changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Security Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Security Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Define types of changes that may impact CIP-005 or CIP-007 security controls.~~ Control the implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007. For those changes: 1.1.1. ~~Prior to change implementation, identify impacted security controls in CIP-005 and CIP-007, except during CIP Exceptional Circumstances;~~ ~~1.1.2.~~ Authorize ~~those~~ the change~~s~~; and 1.1.2~~3~~. Verify the required cyber security controls remain implemented as required as a part of the change. ~~from CIP-005 and CIP-007 are not adversely affected.~~ Changes to software include the installation removal, or update of	Examples of evidence may include, but are not limited to, a documented process that ~~defines~~ controls intended changes to software, or intended changes to settings that may ~~impact~~ weaken cyber security controls in CIP-005 and CIP-007, ~~such as but not limited to~~such as: • Operating system (OS) software; • Firmware~~, where no independent OS exists~~; • Commercially available or open-source application software, including application containers; • Custom software installed, including application containers; • Configuration that modifies network accessible logical ports or network accessible services on an Applicable System; • SCI configuration of host affinity control between systems with different

CIP-010-5 Table R1 – Security Configuration Change Management

Part	Applicable Systems	Requirements	Measures
		operating system, firmware, commercial and custom software, and security patches.	impact ratings; • Changes to configurations or settings for an ESP between systems with different impact ratings; • Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations; or • Any other configuration or setting determined by the Responsible Entity. ~~(1.1.1.)~~ ~~• Documentation of the impacted security controls in CIP-005 and CIP-007;~~ (1.1.1~~2~~.) • A change request record and associated authorization for applicable changes; or • Records from a change management system that identifies applicable changes and records of authorization for changes. (1.1.2~~3~~.) • A list of cyber security controls verified ~~or tested~~ along with the dated ~~test~~ results; or • A~~n~~ dated output from cyber security ~~testing~~ tools such as a vulnerability scanner.

CIP-010-5 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS	1.2.1. Prior to implementing an~~y~~ intended change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 and CIP-007 ~~are not adversely affected~~ remain implemented as required; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this	Prior to ~~software~~ the installation of operating systems, ~~(or~~ firmware ~~where no OS exists)~~ software, or software patches ~~version change~~ and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to ~~the baseline change~~ installation or a process which documents the mechanisms in place

CIP-010-5 Table R1 – Security Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	Part Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	source; and 1.3.2. Verify the integrity of the software obtained from the software source.	that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Security Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Security Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Methods to monitor ~~for unauthorized changes~~ at least once every 35 calendar days~~.~~ for unauthorized changes to software, or unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007, per system capability. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs or records from a system that is monitoring for unauthorized changes along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	Applicable Systems	Requirements	Measures
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BES Cyber Systems SCI supporting an Applicable System in this Part	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements of the same type of Cyber System~~s~~ with a configuration of the previous or other existing Cyber System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of any tools used to perform the assessment, or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.
3.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of evidence may include, but are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, ~~and~~ associated ~~Protected Cyber Assets~~PCAs and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	~~The Responsible Entity’s change management process(es) did not include one of the required items listed in 1.1.1 through 1.1.3. (Part 1.1)~~	~~The Responsible Entity’s change management process(es) did not define the types of changes that may impact either CIP-005 or CIP-007 controls. (Part 1.1)~~ ~~OR~~ The Responsible Entity’s change management process(es) does not include ~~two~~ one of the required items listed in 1.1.1 through 1.1.2~~3~~. (Part 1.1); OR The Responsible Entity’s change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity’s change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	~~The Responsible Entity’s management process(es) did not define the types of changes that may impact both CIP-005 and CIP-007 controls. (Part 1.1)~~ ~~OR~~ The Responsible Entity change management process(es) did not include the ~~three~~ two required items listed in 1.1.1 through 1.1.2~~3~~. (Part 1.1) OR The Responsible Entity’s change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. (Part 1.2); OR The Responsible Entity’s change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity neither documented nor implemented any change management process(es) that include required items in Part 1.1 through Part 1.2~~3~~. (Requirement R1)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	N/A	N/A	The Responsible Entity did not document nor implemented a process(es) with methods to monitor for unauthorized changes at least once every 35 calendar days. (Part 2.1); OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1);	The Responsible Entity neither documented nor implemented a process(es) with methods to monitor for at least once every 35 calendar days and neither documented nor investigated detected unauthorized changes. (Part 2.1)
R3.	The Responsible Entity performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity did not implement any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3) OR The Responsible Entity performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity performed an active

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2) OR The Responsible Entity did not perform the active vulnerability assessment of a Cyber System prior to it becoming an Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4.	The Responsible Entity did not manage its Transient Cyber Asset(s) according to Attachment 1, Section 1.1. (Requirement R4) OR The Responsible Entity did not document the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document authorization for TCA managed by the Responsible Entity according to Attachment 1, Section 1.2. (Requirement R4)	The Responsible Entity did not implement the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCA managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4)	The Responsible Entity did not authorize its TCA(s) according to Attachment 1, Section 1.2. (R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	The Responsible Entity did not document or implement one or more plan(s) for TCAs and Removable Media according to Requirement R4. (Requirement R4)

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.
- CIP-010-5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	

CIP-010-5 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution~~ that mitigates the risk of introduction of malicious code~~;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCA(s). This can be included as part of the TCA(s), part of the documentation related to authorization of TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution~~live operating systems from read-only media~~, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, ~~procedures or processes associated with using live operating systems,~~ methods to maintain the known good state of the OS and all software, or system hardening practices. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, controls to maintain the known good state of the OS and all software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, controls to maintain the known good state of the OS and all software by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed of modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5~~4~~

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting ~~BES Cyber Systems~~BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5~~4~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2.~~4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **"Applicable Systems":** Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan"~~ for Project 2019-03~~.

~~**6. Background:** Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**"Applicable Systems" Columns in Tables:**~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~

- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manage changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5~~4~~ Table R1 – Security Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5~~4~~ Table R1 – Security Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5~~4~~ Table R1 – Security Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.1	High ~~I~~impact BCS~~ES Cyber Systems~~ and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~I~~impact BCS~~ES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Develop a baseline configuration, individually or by group, which shall include the following items:~~ Control the implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007. For those changes: 1.1.1. Authorize the changes; and ~~Operating system(s) (including version) or firmware where no independent operating system exists;~~ 1.1.2. Verify the required cyber security controls remain implemented as required as a part of the change. Changes to software include the	Examples of evidence may include, but are not limited to, a documented process that controls intended changes to settings that may weaken cyber security controls in CIP-005 and CIP-007, such as: • Operating system (OS) software; • Firmware; • Commercially available or open-source application software, including application containers; • Custom software installed, including application containers; • Configuration that modifies network accessible logical ports or network accessible services on an Applicable System; • SCI configuration of host affinity

CIP-010-54 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		installation, removal, or update of operating system, firmware, commercial and custom software, and security patches. ~~Any commercially available or open-source application software (including version) intentionally installed;~~ ~~1.1.2. Any custom software installed;~~ ~~1.1.3. Any logical network accessible ports; and~~ ~~1.1.4. 1.1.5. Any security patches applied.~~	control between systems with different impact ratings; - Changes to configurations or settings for an ESP between systems with different impact ratings; - Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations; or - Any other configuration or setting determined by the Responsible Entity. (1.1.1.) - A change request record and associated authorization for applicable changes; or - Records from a change management system that identifies applicable changes and records of authorization for changes. (1.1.2.) - A list of cyber security controls verified along with the dated results; or

CIP-010-5~~4~~ Table R1 – ~~Security~~ Configuration Change Management

Part	Applicable Systems	Requirements	Measures
			• A dated output from cyber security tools such as a vulnerability scanner. ~~• A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or~~ ~~• A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.~~
~~1.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Authorize and document changes that deviate from the existing baseline configuration.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or~~ ~~• Documentation that the change was performed in accordance with the requirement.~~

CIP-010-54 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~1.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.~~	~~An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.~~
~~1.4~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For a change that deviates from the existing baseline configuration:~~ ~~1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;~~ ~~1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and~~ ~~1.4.3. Document the results of the verification.~~	~~An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.~~
1.2~~5~~	High ~~I~~impact BCS~~ES Cyber Systems~~	~~Where technically feasible, for each change that deviates from the existing baseline configuration:~~ 1.2~~5~~.1. Prior to implementing an~~y~~	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of

CIP-010-5~~4~~ Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		intended change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects~~, that models the baseline configuration~~ to ensure that the configuration of required cyber security controls in CIP-005 and CIP-007 ~~are not adversely affected~~ remain implemented as required; and 1.2~~5~~.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.
1.3~~6~~	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated:	Prior to ~~a change~~the installation of operating systems, firmware, software,	An example of evidence may include, but is not limited to a change request

CIP-010-5~~4~~ Table R1 – ~~Security~~ Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	or software patches ~~that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5,~~ and when the method to do so is available to the Responsible Entity from the software source: 1.3~~6~~.1. Verify the identity of the software source; and 1.3~~6~~.2. Verify the integrity of the software obtained from the software source.	record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to ~~the baseline change~~ installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5~~4~~ Table R2 – Security Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5~~4~~ Table R2 – Security Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5~~4~~ Table R2 – Security Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Methods to ~~M~~monitor at least once every 35 calendar days for unauthorized changes to software, or unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007, per system capability. ~~for changes to the baseline configuration (as described in Requirement R1, Part 1.1).~~ Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs or records from a system that is monitoring ~~the configuration~~for unauthorized changes along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5~~3~~ Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5~~3~~ Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-54 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.1	High ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-54 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~I~~impact BES Cyber Systems SCI supporting an Applicable System in this Part	~~Where technically feasible, a~~At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects~~, that models the baseline configuration of the BES Cyber System in a production environment~~; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-5~~4~~ Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High ~~I~~impact BCS ~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System; or • CIP Exceptional Circumstances. ~~adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.~~	An example of evidence may include, but is not limited to: • The output of any tools used to perform the assessment, or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) ~~, a~~that documents ~~listing~~ the date of the assessment performed prior to becoming a new Applicable System. ~~the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.~~

CIP-010-5~~4~~ Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	~~An e~~Examples of evidence may include, but ~~is~~ are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • ~~, a d~~Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems,~~ and~~ associated ~~Protected Cyber Assets~~PCAs and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for ~~Transient Cyber Assets~~TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for ~~Transient Cyber Assets~~TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use ~~Transient Cyber Asset~~TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use ~~Transient Cyber Asset~~TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)~~	~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)~~ The Responsible Entity's change management process(es) does not include one of the required items listed in 1.1.1 through 1.1.3. (Part 1.1); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management	~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)~~ ~~OR~~ The Responsible Entity ~~has~~ change management ~~a~~ process(es) did not include the two required items listed in 1.1.1 through 1.1.3. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. (Part 1.2); OR	The Responsible Entity ~~has not~~neither documented nor implemented any ~~configuration~~ change management process(es) that include required items in Part 1.1 through Part 1.3. (Requirement R1) ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the~~

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
		process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) ~~as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)~~	~~existing baseline configuration. (1.2)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1)~~ ~~OR~~ ~~The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)~~ ~~OR~~ ~~The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1)~~ ~~OR~~ ~~The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~OR~~ ~~The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)~~
R2.	N/A	N/A	The Responsible Entity did not document nor implemented a process(es) with methods to monitor for unauthorized changes at least once every 35 calendar days. (Part 2.1); OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1);~~N/A~~	The Responsible Entity ~~has not~~ neither documented nor implemented a process(es) with methods to monitor for, ~~investigate, and document detected unauthorized changes to the baseline~~ at least once every 35 calendar days and neither documented nor investigated detected unauthorized changes. (Part 2.1)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R3.	The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its ~~a~~Applicable Systems ~~BES Cyber Systems~~. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.2)	The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.2)	The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.2)	The Responsible Entity ~~has~~ did not implement~~ed~~ any vulnerability assessment processes for one of its ~~a~~Applicable ~~BES Cyber~~ Systems. (Requirement R3) OR The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2) OR The Responsible Entity ~~has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but~~ did not perform the active vulnerability assessment ~~in a manner that models an existing baseline configuration of its~~of a Cyber System prior to it becoming an ~~a~~Applicable ~~BES Cyber~~ Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				each of its ~~a~~Applicable ~~BES Cyber~~ Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)
R4.	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not manage its Transient Cyber Asset(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.1. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~ did not implement the Removable Media sections according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not authorize its ~~Transient Cyber Asset~~TCA(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity did not ~~failed to~~ document or implement one or more plan(s) for ~~Transient Cyber Assets~~TCAs and Removable Media according to ~~CIP-010-4,~~ Requirement R4. (Requirement R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Removable Media, but failed to~~did not document the Removable Media sections according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document authorization for ~~Transient Cyber Assets~~ TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (Requirement R4)	~~Removable Media plan, but failed to~~did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~ did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according	~~Removable Media, but failed to~~ did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCAs managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for ~~Transient Cyber Assets~~TCAs managed by a party other than the Responsible Entity according	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections ~~2.~~1.3, ~~2.2~~1.4, and ~~2.3.~~1.5. (Requirement R4)	to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan” ~~for Project 2019-03~~.
- CIP-010-5~~4~~ Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	

CIP-010-4 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. ~~Transient Cyber Asset~~TCA(s) Managed by the Responsible Entity.

1.1. ~~Transient Cyber Asset~~TCA Management: Responsible Entities shall manage ~~Transient Cyber Asset~~TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, ~~to a BES Cyber System,~~ or (3) a combination of both (1) and (2) above.

1.2. ~~Transient Cyber Asset~~TCA Authorization: For each individual or group of ~~Transient Cyber Asset~~TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset~~TCA (per ~~Transient Cyber Asset~~TCA capability):

- Security patching, including manual or managed updates;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;
- ~~Live operating system and software executable only from read-only media;~~
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;
- Application whitelisting; or

- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of ~~Transient Cyber Asset~~TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. ~~Transient Cyber Asset~~TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset~~TCA (per TCA~~Transient Cyber Asset~~ capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of ~~O~~other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code~~use of live operating system and software executable only from read-only media~~;
- Review of system hardening used by the party; or
- Review of ~~O~~other method(s) to mitigate malicious code.

2.3. For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset~~TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code ~~to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets~~, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ~~using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets~~; and

3.2.2. Mitigate the threat of detected malicious code ~~on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets~~.

CIP-010-4 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the ~~Transient Cyber Asset~~TCA(s). This can be included as part of the ~~Transient Cyber Asset plan~~TCA(s), part of the documentation related to authorization of ~~Transient Cyber Asset~~TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of ~~Transient Cyber Asset~~TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution~~live operating systems from read-only media~~, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, ~~procedures or processes associated with using live operating systems, or procedures or processes associated with~~methods to maintain the known good state of the OS and all software, or system hardening practices. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, controls to maintain the known good state of the OS and all software~~processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code~~, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, controls to maintain the known good state of the OS and all software ~~use of live of operating systems or system hardening performed~~ by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
45-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-4
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-4:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards" Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BCSI pertaining to Applicable Systems identified in *CIP-011-4 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High impact BCS and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following:

CIP-011-4 Table R1 – Information Protection Program			
Part	Applicable Systems	Requirements	Measures
	1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part		• Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-4 Table R2 –Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4 Table R2 –Reuse and Disposal

Part	Applicable Systems	Requirements	Measures
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).	Examples of evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

B. Compliance

1. **Compliance Monitoring Process:**

   1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

   1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

   The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

   - The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
   - If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
   - The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

   1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-011-4)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not implement one or more BCSI protection program(s). (Requirement R1) OR The Responsible Entity did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity did not include disposal processes to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity neither documented nor implemented any processes for applicable requirement parts in CIP-011-4 Table R2 –Reuse and Disposal. (Requirement R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~second~~ fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
~~45~~53-day formal comment period with ballot	February 18 – April ~~4~~12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	~~April~~ October 2022
Board adoption	~~May~~ November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled "Project 2016-02 Draft 4~~3~~ Definitions"

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-4

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers:**
All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-011-4:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards" Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BCSI pertaining to Applicable Systems identified in *CIP-011-4 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s).

CIP-011-4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-4 Table R2 –Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4 Table R2 –Reuse and Disposal			
Part	Applicable Systems	Requirements	Measures
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).	Examples of evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

B. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-011-4)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td>R1</td><td>N/A</td><td>N/A</td><td>The Responsible Entity did not implement one or more BCSI protection program(s). (Requirement R1)
OR
The Responsible Entity did not implement at least one method to identify BCSI. (Part 1.1)
OR
The Responsible Entity did not implement at least one method to protect and securely handle BCSI. (Part 1.2)</td><td>The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)</td></tr>
<tr><td>R2</td><td>N/A</td><td>The Responsible Entity did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)</td><td>The Responsible Entity did not include disposal processes to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)</td><td>The Responsible Entity neither documented nor implemented any processes for applicable requirement parts in CIP-011-4 Table R2 –Reuse and Disposal. (Requirement R2)</td></tr>
</table>

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 – September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 22
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 Draft 4 Definitions”

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:** CIP-011-4~~3~~

3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

   4.1.4 Generator Owner

   4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-4~~3~~:

4.2.3.1 Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5.1a~~7 identification and categorization processes.

4.3. **"Applicable Systems":** Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards" Implementation Plan ~~for CIP-011-3~~.

~~**6. Background:** Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~"Applicable Systems" Columns in Tables:~~

~~Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for ~~BES Cyber System Information (~~BCSI~~)~~ pertaining to ~~“~~Applicable Systems~~”~~ identified in *CIP-011-4~~3~~ Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-4~~3~~ Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-4~~3~~ Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4~~3~~ Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of ~~acceptable~~ evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity’s information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity’s information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity’s information protection program.

CIP-011-4~~3~~ Table R1 – Information Protection Program

Part	Applicable Systems	Requirements	Measures
1.2	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or

CIP-011-4~~3~~ Table R1 – Information Protection Program			
Part	Applicable Systems	Requirements	Measures
			- Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-4~~3~~ Table R2 –~~ BES Cyber Asset~~ Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4~~3~~ Table R2 –~~ BES Cyber Asset~~ Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4~~3~~ Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BCS~~BES Cyber Systems~~ and their associated: 1. EACMS; 2. PACS; and 3. PCA	~~Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action~~Methods to prevent the unauthorized retrieval of BCSI from ~~the Cyber Asset data storage media~~Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).	Examples of ~~acceptable~~ evidence may include, but are not limited to, the following: - Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or - Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

CIP-011-4~~3~~ Table R2 – ~~BES Cyber Asset~~ Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~2.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.~~	~~Examples of acceptable evidence may include, but are not limited to, the following:~~ ~~• Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or~~ ~~• Records of actions taken to prevent unauthorized retrieval of BCSI prior to the disposal of an applicable Cyber Asset.~~

B. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-011-4~~3~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~documented, but~~ did not~~,~~ implement one or more BCSI protection program(s). (Requirement R1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity ~~implemented one or more documented processes but~~ did not include processes for reuse as to prevent the unauthorized retrieval of BCSI from	The Responsible Entity ~~implemented one or more documented processes but~~ did not include disposal ~~or media destruction~~ processes to prevent the unauthorized retrieval of BCSI from an	The Responsible Entity ~~has not~~neither documented nor implemented any processes for applicable requirement parts in CIP-011-4~~3~~ Table R2~~3~~ – ~~BES Cyber Asset~~ Reuse and Disposal. (Requirement R2)

R #	Violation Severity Levels (CIP-011-4~~3~~)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		~~the BES Cyber Asset~~an Applicable System. (Part 2.1)	Applicable System~~the BES Cyber Asset~~. ~~-~~(Part 2.~~2~~1)	

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled "Project 2016-02 Draft 4 Definitions"

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS).

4. **Applicability:**

    4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

        4.1.1. **Balancing Authority**

        4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

            4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

                4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

                4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

            4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

            4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

        4.1.3. **Generator Operator**

        4.1.4. **Generator Owner**

        4.1.5. **Reliability Coordinator**

        4.1.6. **Transmission Operator**

        4.1.7. **Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-3:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable systems listed in Requirement R1 to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring applicable systems listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited

to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's supply chain cyber risk management plan(s) did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1. OR The Responsible Entitiy's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in Requirement R1.
R2.	The Responsible Entity did not implement one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity did not implement the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1, and did not implement the use of process(es) for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				procuring applicable systems as specified in Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in Requirement R2.
R3.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 16th calendar month since the previous review.	The Responsible Entity exceeded the 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 17th calendar month since the previous review.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 18th calendar month since the previous review.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan”
- CIP-013-3 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~third~~ fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
~~45~~53-day formal comment period with ballot	February 18 – April 12~~4~~, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October~~April~~ 2022
Board adoption	~~May~~ November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled "Project 2016-02 Draft ~~3~~4 Definitions"

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

- **4.2.1.** **Distribution Provider:** One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:
  - **4.2.1.1.** Each UFLS or UVLS System that:
    - **4.2.1.1.1.** Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
    - **4.2.1.1.2.** Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - **4.2.1.2.** Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - **4.2.1.3.** Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - **4.2.1.4.** Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.
- **4.2.2.** **Responsible Entities listed in 4.1 other than Distribution Providers:** All BES Facilities.
- **4.2.3.** **Exemptions:** The following are exempt from Standard CIP-013-3:
  - **4.2.3.1.** Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.
  - **4.2.3.2.** Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).
  - **4.2.3.3.** Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. **Effective Date:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable systems listed in Requirement R1 to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring applicable systems listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited

to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's supply chain cyber risk management plan(s) did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1. OR The Responsible Entitiy's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in Requirement R1.
R2.	The Responsible Entity did not implement one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity did not implement the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1, and did not implement the use of process(es) for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				procuring applicable systems as specified in Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in Requirement R2.
R3.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 16th calendar month since the previous review.	The Responsible Entity exceeded the 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 17th calendar month since the previous review.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 18th calendar month since the previous review.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review.

D. Regional Variances

None.

E. Associated Documents

- See "Project 2016-02 Modifications to CIP Standards Implementation Plan"
- CIP-013-3 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fourth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	October 2022
Board adoption	November 2022

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed of modified terms titled “Project 2016-02 Draft 4 Definitions”

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3~~2~~**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.3. Generator Operator

    4.1.4. Generator Owner

    4.1.5. Reliability Coordinator

    4.1.6. Transmission Operator

    4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-3~~2~~:

4.2.3.1. Cyber ~~Assets~~ Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~ Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan" ~~for Project 2019-03~~.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact ~~BES Cyber Systems~~BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), ~~and~~ Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable ~~BES Cyber S~~systems ~~and their associated EACMS and PACS~~listed in Requirement R1 to identify and assess cyber security risk(s) to the ~~Bulk Electric System~~BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring ~~BES Cyber~~applicable ~~S~~systems~~, and their associated EACMS and PACS,~~listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor~~for use in the BES Cyber System and their associated EACMS and PACS~~; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the

scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's ~~developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the~~ supply chain cyber risk management plan(s) ~~do~~did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's ~~developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the~~ supply chain cyber security risk management plan(s) ~~do~~did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's ~~developed one or more documented supply chain cyber security risk management plan(s), but the~~supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~ applicable systems as specified in Part 1.1.~~,~~ OR The Responsible Entitiy's supply chain cyber security risk management ~~or the~~ plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and~~	The Responsible Entity's ~~developed one or more documented supply chain cyber security risk management plan(s), but the~~ supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement ~~of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~ applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~ applicable systems as specified in Part 1.2. OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~PACS,~~ applicable systems as specified in Part 1.2.	The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in ~~the~~ Requirement R1.
R2.	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but~~ did not implement one	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but~~ did not implement two	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or~~ did not implement the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~ applicable systems as	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s), but~~ did not implement the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~ applicable systems as specified in ~~Requirement R1~~ Part 1.1, and did not implement the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~ applicable systems as

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the parts in ~~Requirement R1~~ Part 1.2.1 through Part 1.2.6.	or more of the parts in ~~Requirement R1~~ Part 1.2.1 through Part 1.2.6.	specified in ~~Requirement R1~~ Part 1.2.	specified in ~~Requirement R1~~ Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in ~~the~~ ~~r~~Requirement R2.
R3.	The Responsible Entity exceeded 15 calendar months by reviewing~~ed~~ and obtaining~~ed~~ CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than~~~~15 calendar months~~ ~~but less than or equal to~~in the 16th calendar month~~s~~ since the previous review. ~~as specified in the Requirement~~	The Responsible Entity exceeded the 15 calendar months by reviewing~~ed~~ and obtaining~~ed~~ CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than but less than or equal to~~ in the 17th calendar month~~s~~ since the previous review ~~as specified in the Requirement~~.	The Responsible Entity exceeded 15 calendar months by reviewing~~ed~~ and obtaining~~ed~~ CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than 17 calendar months but less than or equal to~~in the 18th calendar month~~s~~ since the previous review ~~as specified in the Requirement~~.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review ~~as specified in the Requirement~~.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan” ~~for Project 2019-03~~
- CIP-013-3~~2~~ Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards
Virtualization | Draft 4

Applicable Standard(s)

- Reliability Standard CIP-002-7 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-Y – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-8 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-8 – Cyber Security – BES Cyber System Logical Isolation
- Reliability Standard CIP-006-7 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-7 – Cyber Security – System Security Management
- Reliability Standard CIP-008-7 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-5 – Cyber Security – Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-4 – Cyber Security – Information Protection
- Reliability Standard CIP-013-3 – Cyber Security – Supply Chain Risk Management
- Proposed new or modified terms listed in the "CIP Definitions Posting Document (Project 2016-02)"

  These standards and Definitions of Terms used in the versions listed above of the CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

  These standards and new and modified terms used in the standards above will be referenced as the "Revised CIP Standards and Definitions" within the Implementation Plan.

Requested Retirement(s)

- Reliability Standard CIP-002-6 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-8 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-7 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)
- Reliability Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems

- Reliability Standard CIP-007-6 – Cyber Security – System Security Management
- Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-3 – Cyber Security – Information Protection
- Reliability Standard CIP-013-2 – Cyber Security – Supply Chain Risk Management

These standards and definitions used in the versions listed above will be referenced as the "Requested CIP Retired Standards and Definitions" within the Implementation Plan.

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved or retired before the Applicable Standard become effective:

- BES Cyber Asset (BCA)
- BES Cyber System (BCS)
- BES Cyber System Information (BCSI)
- CIP Senior Manager
- Cyber Assets
- Cyber Security Incident
- Cyber System
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate System
- Management Interface
- Physical Access Control Systems (PACS)
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Removable Media

- Reportable Cyber Security Incident
- Shared Cyber Infrastructure (SCI)
- Transient Cyber Asset (TCA)
- Virtual Cyber Asset (VCA)

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions. The intent of the Compliance Dates for Early Adoption of Revised CIP Standards and Definitions section is to permit Responsible Entities the option to comply with the Revised CIP Standards and Definitions prior to the Effective Date. While the Revised CIP Standards and Definitions are designed to be backwards compatible with perimeter-based security, some Responsible Entities may elect to comply early to leverage different security options associated with zero trust architecture.

Effective Date and Phased-in Compliance Dates

The Effective Dates for the Revised CIP Standards and Definitions are provided below. As noted in the General Considerations section above, the standard drafting team determined to clarify initial performance of periodic requirements and permit Responsible Entities to comply with the Revised CIP Standards and Definitions prior to the effective date. These provisions also are provided below.

Revised CIP Standards and Definitions

Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the

---

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the date the Revised CIP Standards and Definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards and Definitions.

Compliance Dates for Early Adoption of Revised CIP Standards and Definitions

A Responsible Entity may elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. In such a case, the Responsible Entity shall select one of the following Early Adoption Dates and shall notify the applicable Regional Entities of their selected Early Adoption Date within fifteen (15) calendar days after their selected Early Adoption Date:

Early Adoption Date
Option 1: First day of the first calendar quarter that is six (6) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 2: First day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 3: First day of the first calendar quarter that is eighteen (18) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions

Responsible Entities must comply with applicable Requested CIP Retired Standards and Definitions until their selected Early Adoption Date. All Responsible Entities, regardless of whether or not they selected an Early Adoption Date, must comply with the Revised CIP Standards and Definitions by the Effective Date.

Planned or Unplanned Changes

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-7, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-7, Attachment 1, criteria.

For unplanned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirement not applicable to Medium impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Retirement Date

Requested CIP Retired Standards and Definitions

The Requested CIP Retired Standards and Definitions shall be retired immediately prior to the effective date of the Revised CIP Standards and Definitions in the particular jurisdiction in which the Revised CIP Standards and Definitions are becoming effective.

CIP Definitions

Project 2016-02 Modifications to CIP Standards

Virtualization – Draft 4

The standard drafting team (SDT) is seeking comment on the following new, modified, or retired terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

~~Table 1:~~ Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the ~~r~~Reliable ~~o~~Operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS) **Update is Acronym only.**	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	
BES Cyber System Information	Information about the BES Cyber System that could be used to gain	Information about the BES Cyber System or Shared Cyber

~~Table 1:~~ Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
(BCSI)	unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	Infrastructure that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC ~~CIP Standards, CIP-002 through CIP-011~~Critical Infrastructure Protection Standards.
Cyber Assets	Programmable electronic devices, including the hardware, software, and	Programmable electronic devices, excluding Shared Cyber

~~Table 1:~~ Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	data in those devices.	Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: • For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, ~~or~~ (3) an Electronic Access Control or Monitoring System; or (4) Shared Cyber Infrastructure; or • Disrupts or attempts to disrupt the operation of a BES Cyber System.
Cyber System ***New Definition***		A group of one or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Intermediate Systems.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication	An electronic policy enforcement point or a Cyber Asset interface on an EACMS ~~on an Electronic Security~~

~~Table 1:~~ Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
	between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	~~Perimeter~~ that ~~allows~~controls routable communication to and from one or more BES Cyber Systems and their associated Protected Cyber Assets (PCAs) ~~between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter~~.
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System ~~from a Cyber Asset that is outside of its associated~~through its ~~Electronic Security Perimeter~~ Electronic Security Perimeter via a bi-directional routable protocol connection.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more EAPs.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated electronic access by a person ~~employing a remote access client or other remote access technology~~ using a routable protocol:~~.~~ • To a Cyber System protected by an ~~Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's~~ Electronic Security Perimeter(s) (ESP); • That is converted by the Responsible Entity to a non-routable protocol to a Cyber System; or

~~Table 1:~~ Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
		• To a Management Interface of Shared Cyber Infrastructure. Interactive Remote Access does not include: • Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; • Communication that originates from an Intermediate System; or • System-to-system process communication. ~~at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.~~
Intermediate System~~s~~	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users. ~~A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be~~

~~Table 1:~~ Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
		~~located inside the Electronic Security Perimeter.~~
Management Interface ***New Definition***		An administrative interface that: - Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or - Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or - Configures an Electronic Security Perimeter.
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers	Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber	One or more Cyber Assets or Virtual Cyber Assets that: - ~~connected using a routable protocol~~Are ~~within~~ protected by ~~or on~~ an Electronic Security Perimeter (ESP) but are ~~that is~~ not part of the

~~Table 1:~~ Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
	Assets is equal to the highest rated BES Cyber System in the same ESP.	highest impact BES Cyber System ~~within~~ protected by the same ~~Electronic Security Perimeter~~ESP; or • ~~.~~Share CPU or memory resources with any part of the ~~The impact rating of Protected Cyber Assets is equal to the highest rated~~ BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated ~~in the same ESP~~in an environment that isolates routable connectivity from BES Cyber Systems;~~.~~ Excluding Transient Cyber Assets.
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, Shared Cyber Infrastructure, a network ~~within~~ protected by an ESP, or a Protected Cyber Asset. ~~Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a	A Cyber Security Incident that compromised or disrupted: • A BES Cyber System that performs one or more reliability tasks of a functional entity;

~~Table 1:~~ Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	• An Electronic Security Perimeter of a high or medium impact BES Cyber System; ~~or~~ • An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or • Shared Cyber Infrastructure supporting a BES Cyber System.
Shared Cyber Infrastructure (SCI) ***New Definition***		One or more programmable electronic devices, including the software that shares the devices' resources, that: • Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or • Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization. SCI does not include the supported VCAs or Cyber Assets with which it

~~Table 1:~~ Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
		shares its resources.
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. • Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	A Cyber Asset or Virtual Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. ~~directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication)~~connected for 30 consecutive calendar days or less ~~to a~~: • ~~BES Cyber Asset,~~ • To a network ~~within~~ protected by an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a: • BES Cyber Asset, or • Shared Cyber Infrastructure, or • PCA associated with high or

~~Table 1:~~ Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
		medium impact BES Cyber Systems. Virtual machines hosted on a physical TCA are treated as software on that physical TCA. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Virtual Cyber Asset (VCA) ***New Definition***		A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure.~~;~~ VCAs do not include: • Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems; • Dormant file based images that contain operating systems or firmware; and • SCI or Cyber Assets (CA) that host VCAs. Application containers are considered software of VCAs or CAs.

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards
Virtualization – Draft 4

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on the **CIP Virtualization suite of Standards** by **8 p.m. Eastern, Friday, September 30, 2022.**

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Jordan Mallory (via email) or at 404-446-2589.

Background Information

Project 2016-02 (1) addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and (2) considers the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for Standard Drafting Team Consideration (V5TAG Transfer Document).

The V5TAG, which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP Version 5 standards and to support industry's implementation activities. During the V5TAG's activities, it identified certain issues with the CIP Reliability Standards that would be better addressed by a standard drafting team (SDT) for the CIP Reliability Standards. The V5TAG developed the CIP Version 5 Transition Advisory Group Issues for Consideration document to formally recommend that the SDT address these issues and consider modifications to the standard language during the standards development process.

Summary of Changes Overview

The SDT reviewed all comments and made modifications to the Reliability Standards and Definitions accordingly. There are currently two drafting teams working on modifications to CIP-003-8. The NERC Project 2016-02 SDT is posting its modifications as CIP-003-Y to differentiate its work from the Supply Chain Low drafting teams (Project 2020-03) modifications, which has posted CIP-003-X.

In addition, the proposed new and revised definitions are not balloted separately but are being balloted via the standards. As such, when voting on the standards, ballot body participants will also be voting on the proposed new and revised definitions used in those standards. The definitions are posted in one document among the other ballot materials. While CIP-002, CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 passed ballot during the draft 3 posting, the SDT will be balloting all standards again based on updated definitions.

Below are questions for which the SDT is seeking industry input. In order to allow the SDT to sort comments received by topic, the SDT respectfully requests comments be submitted with the respective question topic. The SDT thanks all stakeholders for your time and responses during this comment period.

Questions

1. The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

2. The SDT modified other definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

3. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

4. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

5. The SDT has used phrasing such as “SCI supporting an Applicable System from this Part” in the Applicable Systems column across many of the standards. Is it clear that this scopes the requirements for SCI to match the system(s) it hosts?

   ☐ Yes
   ☐ No

   Comments:

6. The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

7. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes or scoping clarifications related to SCI. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

8. The SDT has revised the Implementation Plan to include 3 defined early adoption dates as options should Responsible Entities choose to do so. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

9. Please provide any additional comments for the standard drafting team to consider, if desired.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Technical Rationale

Project 2016-02 Modifications to CIP Standards

New and Modified Terms, and Exemption Language Used in NERC Reliability Standards

Proposed Modified Terms:

BES Cyber Asset (BCA)

A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Rationale

The BCA definition is changing to allow for BCA to be either Cyber Assets (hardware included) or Virtual Cyber Assets (VCA) (software only virtual machines without the underlying hardware). See the VCA and Shared Cyber Infrastructure (SCI) definition below.

BES Cyber System Information (BCSI)

Information about the BES Cyber System or Shared Cyber Infrastructure that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

Rationale

Conforming changes such that BCSI includes information about SCI.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Standards.

Rationale

Remove explicit reference to the CIP standards as only "CIP-002 through CIP-011" as the body of CIP standards has grown beyond CIP-011. As an example, the CIP Senior Manager also has requirements within CIP-013.

Cyber Assets

Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices;. Application containers are considered software of VCAs or Cyber Assets. VCAs are not considered software or data of Cyber Assets.

Rationale

Modified to explicitly exclude SCI from the definition of Cyber Asset such that SCI is a different hardware class on which the other VCAs of differing impact levels execute. SCI is defined separately such that it can be the object of additional requirements based on its unique risks. The definition is also modified to clarify that 'Application containers' (i.e., portable, packaged applications) are considered software of a Cyber Asset (or VCA), though they may have some characteristics of a VCA. Executing instances of VCAs are not to be considered simply software or data of the Cyber Asset.

Cyber Security Incident

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System, or (4) Shared Cyber Infrastructure; or
- Disrupts or attempts to disrupt the operation of a BES Cyber System.

Rationale

Modified to add SCI to the scope of compromised or attempted compromise systems.

Electronic Access Control or Monitoring Systems (EACMS)

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or Shared Cyber Infrastructure. This includes Intermediate Systems.

Rationale

Modified to add VCA and SCI as two other forms that an EACMS can take and add SCI as an object of the access control or monitoring.

Electronic Access Point (EAP)

An electronic policy enforcement point or a Cyber Asset interface on an EACMS that controls routable communication to and from one or more BES Cyber Systems and their associated PCAs.

Rationale

As network security moves deeper into the infrastructure, it's no longer necessary to prescribe that network security be performed only at a 'Cyber Asset interface on an ESP'; at one point on a network edge. Zero Trust, for example, highly distributes the network security model and is not perimeter-based, and this is incorporated through the addition of "electronic policy enforcement point or". With the added flexibility in CIP-005 to adopt these models in addition to the traditional Electronic Security Perimeter (ESP) model, the term EAP is being modified to allow for electronic policy enforcement points and no longer prescribes an architecture. The "one or more" and the "associated PCAs" have been added to clarify that EAPs can control communications to a group and not required per individual system.

External Routable Connectivity (ERC)

The ability to access a BES Cyber System through its ESP via a bi-directional routable protocol connection.

Rationale

The ERC definition is changing to allow for zero trust or other network models that are not strictly perimeter or network-border based, thus not having concepts of "inside" or "outside". These concepts are replaced with the language "through its ESP" so that it does not imply a prescriptive network security model. The ERC term is used throughout the CIP Standards within the Applicable Systems column as a scoping mechanism based on the inherent risk associated with External Routable Connectivity as well as to limit the scope of requirements that would require ERC to function. The SDT is maintaining this use of ERC, but also clarifying the relationship between ERC and Interactive Remote Access (IRA) in that a non-routable, serial only BCS (thus with no ESP) may have IRA through a subsequent IP/serial conversion (see changes to IRA definition).

Electronic Security Perimeter (ESP)

A logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more EAPs.

Rationale

The traditional network border ESP remains a valid network security model, however it is no longer the only prescribed model as CIP-005 allows other access control models that are not based on network perimeters such as Zero Trust architectures. The proposed ESP definition retains its current definition but appends "or a logical boundary defined by one or more EAPs" to incorporate models that move away from implicit trust within network perimeters and using network location as a primary factor in access control decisions. In these models, the perimeter shrinks to increasingly more granular levels, potentially down to a process or resource level on a BCS. The proposed definition allows for an ESP to be (a) a border surrounding an isolated network that has no external connectivity and thus no EAPs, (b) static point(s) on a network boundary such as a traditional firewall as an EAP that is enforcing access policies or configurations (e.g., firewall rulesets), (c) many dynamic, short-lived, session-level 'perimeters' established at time of access that are network independent (e.g., users to resources, for example), or (d) hybrid implementations combining elements of both.

The SDT has kept the 'logical border' concept for the "surrounding a network" ESP and used the language "logical boundary" for zero trust models. A 'border' does indeed surround an object, in this case a network, but a 'boundary' may not surround or enclose, it's a line that can be crossed, such as a policy enforcement point controlling access to a resource. The SDT has also updated language in the standards to remove concepts such as 'inside' an ESP and replaced that with more inclusive phrases such as 'protected by' an ESP.

Interactive Remote Access (IRA)

User-initiated electronic access by a person using a routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter (ESP);
- That is converted by the Responsible Entity to a non-routable protocol to a Cyber System; or
- To a Management Interface of Shared Cyber Infrastructure.

Interactive Remote Access does not include:

- Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs;
- Communication that originates from an Intermediate System; or
- System-to-system process communication.

Rationale

The proposed IRA definition changes in two fundamental ways: (1) to incorporate IRA situations where users outside of any of the Responsible Entity's ESPs have interactive access, using a routable protocol, to a non-routable (e.g., serial) Cyber System through a subsequent IP to serial conversion, and (2) to include the Management Interfaces of SCI as targets of IRA. The references to ownership of the remote client have been removed as they are immaterial to the definition of IRA.

The definition begins with "User-initiated electronic access by a person using a routable protocol" to match the human interactive nature of the access to the requirements that secure such access in CIP-005 R2. For example, a batch process cannot read a multi-factor token and enter its displayed code; that security control is designed for interactive humans initiating a remote access session. Also note the person is using a routable protocol to initiate the access.

The definition outlines three targets of IRA:

1) "To a Cyber System protected by an Electronic Security Perimeter (ESP)" covers the typical Cyber System that is connected to a network via a routable protocol and thus is protected by an ESP. In this instance, the remote user is using a routable protocol and is accessing a Cyber System on a routable protocol network, for example in a typical LAN-WAN-LAN, end to end routable protocol communication.

2) "That is converted by the Responsible Entity to a non-routable protocol to a Cyber System" clarifies as IRA scenarios where the user is using a routable protocol to a site where the Responsible Entity then connects that session (e.g., using a gateway or terminal server) to a device's non-routable serial port to provide interactive remote access to the user. A common example is connecting a serial port on a digital relay in a substation to a terminal server or gateway device which is then connected to a routable network in the substation for the purpose of granting a remote user interactive access to the relay without traveling to the substation. This 2nd target of the definition now clarifies this is IRA even though the device itself may not have an ESP if it is only connected serially.

   The phrase "converted *by the Responsible Entity*" clarifies certain situations that may involve more than one entity and is best described by an example. Entity 1 has a BCS in a substation or generating resource that Entity 2, a Control Center, needs to access. Entity 2 provides a circuit to Entity 1's site and provides Entity 1 with a serial cable to connect to their BCS. This phrase clarifies that Entity 1 does not require detailed architectural knowledge of what Entity 2 does upstream with the data once delivered to the interface if Entity 1 does not do any conversion to routable protocols. If Entity 2 does convert to routable protocols and does provide IRA, then Entity 2 implements the IRA security controls on their routable protocol portion.

3) "To a Management Interface of Shared Cyber Infrastructure" adds the Management Interface of an SCI as a valid target of IRA.

The definition then has three exclusions of scenarios that are not IRA:

1) "Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs" carries forward this exclusion from previous definitions and is intended to exclude, for example, the scenario of a Control Center operator within one of the Responsible Entity's ESPs interacting with field devices within its other ESPs, because for it to meet the IRA definition, IRA originates from somewhere other than one of the Responsible Entity's protected ESPs.
2) "Communication that originates from an Intermediate System" prevents the 'hall of mirrors' situation where an Intermediate System would need its own Intermediate System, ad infinitum.
3) "System-to-system process communication" carries forward this exclusion from previous definitions to clarify that a process that cannot for instance perform multi-factor authentication using tokens or biometrics is not IRA.

Note that the definition uses the more generic term Cyber Systems. This is in keeping with using the glossary as a dictionary that merely defines a term, in this case a type of access, but does not create or scope CIP requirements within the definition. The scope of access that requires an Intermediate System is in CIP-005 R2's requirement language.

Intermediate Systems

One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.

Rationale

This definition is changing to remove requirement language (i.e., where an Intermediate System must reside) embedded within the definition. That language has been moved to CIP-005 Requirement R2 Part 2.6.2 within a mandatory requirement. The definition was also updated from a Cyber Asset focus to an EACMS focus to include other forms (i.e., VCA) the Intermediate System may take.

Physical Access Control Systems (PACS)

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Rationale

Modified to add VCA and SCI as two other forms that a PACS can take.

Physical Security Perimeter (PSP)

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Rationale

The PSP definition is changing to add SCI as type of device to be included within a PSP.

Protected Cyber Asset (PCA)

One or more Cyber Assets or Virtual Cyber Assets that:

- Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System protected by the same ESP; or
- Share CPU or memory resources with any part of the BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems;

Excluding TCAs.

Rationale

The PCA definition exists to identify other Cyber Assets or VCAs that must be protected by various CIP requirements due to what they share with a BES Cyber System. This sharing could allow the PCA to be a ‘pivot point’, a location from which to access the BCS. In the past, this sharing was limited to local network connectivity; the PCA being a network peer within the same ESP. With virtualization there is now another aspect of sharing and the PCA definition is being updated to include “share CPU or memory resources with any part of the BES Cyber System” to mitigate the risks of hardware-based vulnerabilities (e.g., Spectre, Meltdown, Rowhammer, etc.) on Shared Cyber Infrastructure. Since virtualization can allow systems of differing trust levels to simultaneously execute on the same hypervisor servers in the hardware underlay and thus share the same CPU and memory resources, this addition to the PCA definition requires that those

VCAs that do share CPU and memory resources with a BCS become associated PCA's of the BCS. This provides the high water marking of VCAs sharing a single hypervisor's CPU or memory resources. Affinity rules can be used within the virtualization configuration to prevent this situation and keep other VCAs of differing impact levels from becoming associated PCAs. Finally, the definition is being modified to account for "remediation VLAN" automation of security controls where a VCA may instantiate in a logical network reserved for vulnerability assessment and updates (OS patches, AV updates, etc.) that isolates its connectivity during the remediation process. Even though it may share CPU/memory resources during the remediation, the intent is to exclude the VCA from becoming a PCA while temporarily in this state as its being updated prior to being connected to its production network.

Removable Media

Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, Shared Cyber Infrastructure, a network protected by an ESP, or a Protected Cyber Asset.

Rationale

The Removable Media definition is being updated to add SCI as a target of the Removable Media connection and incorporate the new ESP definition.

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BES Cyber System;
- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or
- Shared Cyber Infrastructure supporting a BES Cyber System.

Rationale

This definition is being modified to add compromised or disrupted SCI supporting a BCS as a target.

Transient Cyber Asset (TCA)

A Cyber Asset or Virtual Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. connected for 30 consecutive calendar days or less:
    a. to a network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or

b. directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a:
    i. BES Cyber Asset,
    ii. Shared Cyber Infrastructure, or
    iii. Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Virtual machines hosted on a physical TCA are treated as software on that physical TCA. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Rationale

The TCA definition is being updated to add VCA as a form a TCA can take. The SDT is addressing two different transient connection scenarios.

The first scenario is a physical TCA such as a laptop. These TCA's may require older, 32-bit software and OS to connect to and configure older equipment in the field. These are often executed within VM 'player' environments on the physical TCA. The SDT asserts these packaged environments in an image file on a physical TCA should not be considered their own distinct virtual TCA and included the statement "Virtual machines hosted on a physical TCA are treated as software on that physical TCA." The SDT asserts that a user that is authorized to use the physical TCA should not be required to be separately authorized to execute the software they need to use on the TCA, simply because it's in an image file and executed in a VM "player" type environment on the TCA. The SDT also asserts that if the user 'checks out' a physical laptop to perform a task, it should not be a standard violation if they do not also 'check out' any VM images residing on that physical TCA's disk. The intent is that physical TCA is considered a 'unit' to perform a job and not several distinct TCAs on one laptop. Corresponding clarifications have been made to the methods in CIP-003 and CIP-010 used to mitigate the risks of TCA software.

The second scenario is a more recent phenomenon where a service vendor (e.g., a pen-tester or security firm) may send an entity a VCA image (e.g., a vulnerability scanner instance) to temporarily instantiate within their virtualization environment. This VCA may only exist for a few hours and is functionally no different than the vendor bringing a physical laptop and connecting it to a physical network switch to perform the same task as a TCA. This transient VCA is not a part of the entity's CIP program and is treated as a TCA. This also handles VCAs the entity creates for typical TCA uses but are normally dormant on the same hardware as the BCS (e.g., a VCA with Wireshark for troubleshooting network issues within a virtualized infrastructure).

Additionally, SCI was added as a target to which TCA's can be directly connected.

Proposed New Terms:

Cyber System

A group of one or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.

Rationale

This proposed new term is used to simplify applicability when referring in the standards or other definitions to all the forms an object may take (CA, VCA, or SCI). If other forms are needed in the future, their addition to this one definition can reduce needed edits throughout the standards.

Management Interface

An administrative interface that:

- Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or
- Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or
- Configures an Electronic Security Perimeter;

Rationale

This term is being defined so that requirements can be addressed to SCI and EACMS Management Interfaces to target the unique risks for virtualized environments presented by unrestricted access to the Management Interfaces for such environments. With 'infrastructure as a service' (IaaS) environments, the management consoles can not only be used to create, but also to destroy or reconfigure virtual servers, networks, switches, firewalls, etc. The term also includes interfaces commonly known as ILO (Integrated Lights Out), that can be used to remotely access the console. It also includes interfaces used to configure an ESP (such as on firewalls or a network switch that is enforcing an ESP between different logical networks (e.g., VLANs).

Shared Cyber Infrastructure (SCI)

One or more programmable electronic devices, including the software that shares the devices' resources, that:

- Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber System (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or
- Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.

SCI does not include the supported VCA or Cyber Assets with which it shares its resources.

Rationale

The SCI definition is being created to separate the underlying hardware from VCAs in the situation where the shared hardware resources support VCAs of varying impact levels. This allows security requirements to be targeted to SCI to address the unique risks of shared hardware. There are many requirements that now include the newly defined term SCI in the "Applicable Systems" column to maintain security level parity with traditional Cyber Assets.

Beyond security level parity with protecting a typical hardware based Cyber Asset, the SCI can have a more significant impact in a virtualized environment since it can host, and therefore impact, multiple virtualized systems of varying impact levels. Because of this capability, some additional controls only apply to SCI, such as the management plane isolation required by the proposed CIP-005. Addressing these unique risks requires separation of the hardware underlay into a separate definition.

The phrase "SCI does not include the supported VCA or Cyber Assets with which it shares its resources" is included to clarify that, for example, electronic access to a hosted VCA by a user is not electronic access to the SCI on which it executes.

Of note is that shared network devices are not in the scope of this definition. Since network switches and firewalls share their resources by nature, this exclusion avoids pulling all network hardware into scope as SCI. However, network switches and other hardware that does enforce an ESP, such as a network switch configured to host different VLANs to which systems of differing impact levels are connected, comes into scope as an EACMS.

Virtual Cyber Asset (VCA)

A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset, Electronic Access Control or Monitoring System, Physical Access Control System, Protected Cyber Asset, or Shared Cyber Infrastructure. VCAs do not include:

- Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems;
- Dormant file based images that contain operating systems or firmware; and
- SCI or Cyber Assets that host VCAs.

Application containers are considered software of VCAs or Cyber Assets.

Rationale

The NERC Glossary definition of Cyber Asset has a direct tie to its hardware and software ("including the hardware, software, and data in the device") and assumes a one-to-one relationship between a device and its software (including the operating system). This affected the definitions of the "Applicable Systems" terms such as BES Cyber Systems (BCS), EACMS, PACS, and Protected Cyber Assets (PCAs) that were all based on the Cyber Asset definition. Because the Reliability Standard is applicable to the aforementioned systems, the security controls for the Cyber Assets also applies to the hardware. The one-to-one relationship between a Cyber Asset and its underlying hardware and software is what virtualization intentionally breaks to increase reliability and resiliency by allowing Virtual Cyber Assets to be abstracted from the hardware and therefore able move to any available hardware out of a pool of resources. The proposed NERC Glossary definition of Virtual Cyber Asset (VCA) allows the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined.

The phrase "currently executing on a virtual machine" is used to clarify that a VCA does not include disk image files that are not currently instantiated or executing and are thus providing no functions or services. Likewise, the definition excludes "logical instances that are being actively remediated…" to allow for automated solutions (such as remediation VLANs) to bring newly instantiated instances into compliance in an isolated environment before they are moved to production networks and begin providing their function or service, at which point they become a VCA.

The phrase "on a virtual machine" is used to clarify that a dedicated, non-virtualized Cyber Asset may have a 'logical instance of an Operating System (OS) or firmware', but that is not a VCA, only a logical instance of an OS or firewall on a virtual machine is a VCA.

The phrase "hosted on a BCA, EACMS, PACS, PCA, or SCI" is to clarify that an entity for an "all-in" scenario can still classify the underlying hardware as one or several of these types, yet the VCA's remain their own object subject to requirements and are not simply "software in the device" as in the Cyber Asset definition.

Examples of Virtual Cyber Assets may include, but are not limited to, logical instances of the following:

- Operating Systems (Virtual Machines (VM));
- Networking devices such as switches, routers, and load balancers;
- Security appliances such as firewalls and VPN concentrators; and
- Helper appliances with logical connectivity (such as malware detection, plugins, etc.).

Proposed Retired Terms:
None

Technical Rationale for Exemptions Section:
Rationale for Exemption 4.2.3.1
The term 'Cyber Assets' was changed to the new proposed term 'Cyber Systems'. Rather than changing this language to a list of all possible forms (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure) as the object of the exemption, the SDT chose to instead use the existing language in the 4.2.3.4 and 4.2.3.5 exemptions such that all five exemptions use a form of 'systems' as their object.

Rationale for Exemption 4.2.3.2 and 4.2.3.3
In 4.2.3.2, the term 'Cyber Assets' was changed to 'Cyber Systems' which is a new proposed glossary addition. Rather than changing these two exemptions to list all possible forms (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure), the SDT chose to define a new term that incorporates all forms and use it within the multiple exemptions and at other points within the standards.

For 4.2.3.3, the ability to move workloads or VM’s seamlessly across different sites for increased resiliency can require different sites to be connected as a flat network without layer 3 ESP’s at each discrete site (e.g., a layer 2 adjacency across the sites). A “Super ESP” as it’s been historically known is created across the sites and thus an exemption based on having a discrete layer 3 ESP at each site no longer works to exclude, for example, the network transport equipment that may belong to carriers. The SDT is including the 4.2.3.3 exemption to further clarify this scenario. Responsible Entities should notice the exemption uses the word “between” – when extending an ESP between geographic locations, CIP-005 requires the confidentiality and integrity protection of the data (typically through encryption) between the relevant PSPs. This exemption then covers the related Cyber Systems “between” those encryption points but does not exclude the endpoints performing the encryption.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — BES Cyber System Categorization

Technical Rationale and Justification for Reliability Standard CIP-002-7

August 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-002-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-002-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-002-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a SDT. The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Attachment 1 – Impact Rating Criteria

Change Rationale:

In the medium impact rating criterion 2.1 referencing shared BCS for commissioned generation, the SDT has proposed a change to incorporate an earlier approved Request For Interpretation (RFI). The RFI was submitted seeking clarification of Criterion 2.1 of Attachment 1 regarding the use of the phrase "shared BES Cyber Systems." The resulting approved interpretation was introduced as Appendix 1 in CIP-002-5.1a.

The SDT incorporated the interpretation into CIP-002-7 Attachement 1 criterion 2.1 by modifying it to reference "each discrete shared BCS" and removed the RFI appendix from the standard.

Former Background Section from Reliability Standard CIP-002-5.1a

The **Background** section has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

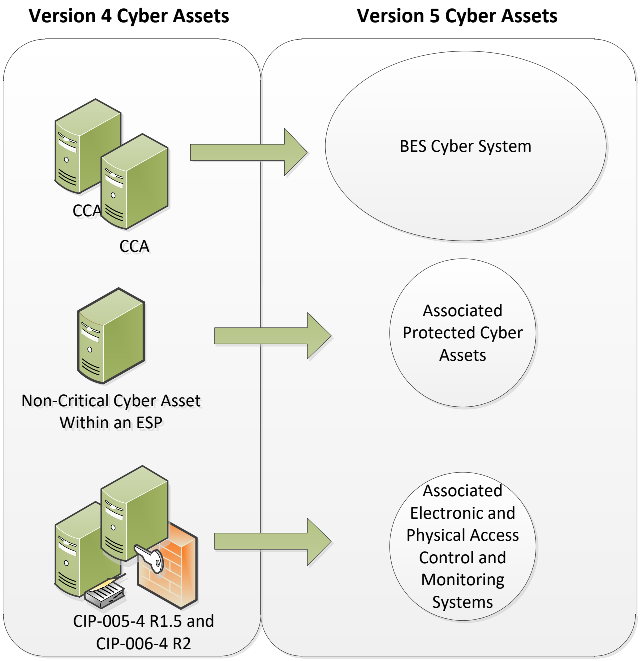
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily

to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS")

Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")

Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA")

Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

Technical Rationale for Reliability Standard CIP-002-5.1a

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from the CIP-002-5.1a standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1a

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints

- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
    - Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)

    - Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
    - Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
    - Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
    - Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO, DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP, TO, DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO, DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC, BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports

the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.

- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.

In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.
- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.
- Criterion 2.13 categorizes as medium impact those BA Control Centers that “control” 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.
- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the “Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface.” This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.
- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:
  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

- 230 kV –> 700 MVA
- 345 kV –> 1,300 MVA
- 500 kV –> 2,000 MVA
- 765 kV –> 3,000 MVA

In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

- For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.
- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.
- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.
- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.
- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.
- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

  In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.
- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

  Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

  BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in

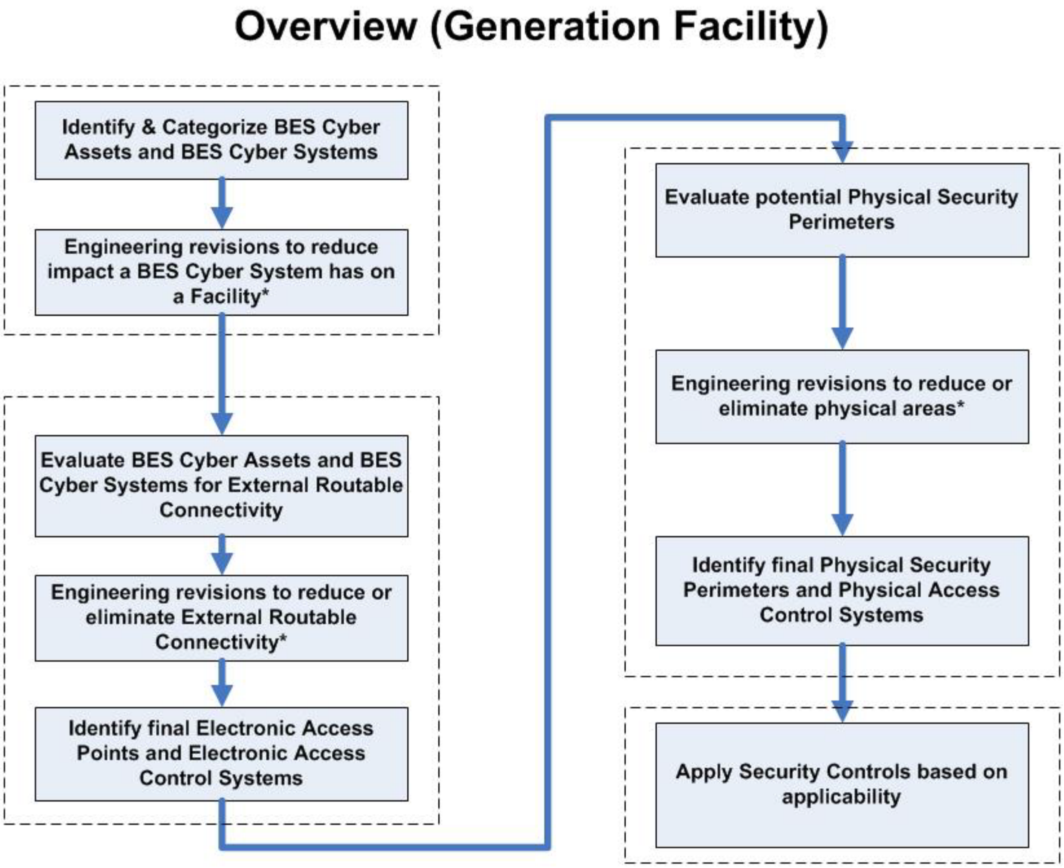
its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



*** - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.**

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Appendix 1

Requirement Number and Text of Requirement
<u>CIP-002-5.1, Requirement R1</u> R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above. 1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset; 1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and 1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required). <u>Attachment 1, Criterion 2.1</u> 2. Medium Impact Rating (M) Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions

Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."

The Interpretation Drafting Team identified the following questions in the RFI:

1. Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?
2. Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?
3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

Responses

Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)

Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:

> The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term “shared” is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.” For criterion 2.2: “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-Y

August 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-003-Y

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-9. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-Y is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document stated, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to shorten applicability statements within the body of CIP standards with “BCS” as the defined acronym for “BES Cyber System”.

Requirement R2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to align security management control requirements with the virtualization changes.

To ensure SCI supporting low impact BCS is afforded equal security controls as the BCS, the SDT added “SCI that supports a low impact BCS”.

Attachment 1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to shorten applicability statements within the body of CIP standards with “BCS” as the defined acronym for “BES Cyber System”.

To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a system(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term system(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Attachment 1 Section 2

Rationale

To ensure virtual infrastructure providing electronic access controls for the low impact BCS is afforded equal physical security controls as the physical Cyber Assets that provide electronic access controls for the low impact BCS, the SDT modified this section to include the Virtual Cyber Asset (VCA) where only Cyber Assets had previously been listed.

Attachment 1 Section 3

Attachment 1 Section 3 Part 3.1

Rationale

Part 3.1(i)

To ensure an asset containing a low impact BCS or an SCI supporting a low impact BCS is afforded equal electronic access controls as the low impact BCS, the SDT added “SCI that supports a low impact BCS and a Cyber System(s) outside the asset containing the low impact BES Cyber System (BCS); or the SCI that supports a low impact BCS””.

To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a Cyber System(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term Cyber System(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Part 3.1(ii) To ensure only necessary inbound and outbound electronic access is permitted for SCI that supports a low impact BCS just as is required for access control to the low impact BCS, the SDT adjusted the language to include communications that are between SCI that supports any part of a low impact BCS and a system(s) outside the asset(s) containing the SCI that supports any part of a low impact BCS.

Part 3.1 (iii) The SDT replaced the undefined 'intelligent electronic devices' with the defined term 'Protection Systems'.

Attachment 1 Section 3 Part 3.2

Rationale

To ensure SCI supporting low impact BCS are afforded equal electronic access controls for Dial-up Connectivity, the SDT added "or SCI that supports a low impact BCS". To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs),, the 'per Cyber Asset capability' was changed to 'per system capability'.

Attachment 1 Section 5

Attachment 1 Section 5 Part 5.1

Rationale

To enable for virtualization technologies and capabilities the SDT added, "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code" as an option in Attachment 1 Section 5 Part 5.1.

Attachment 1 Section 5 Part 5.2

Rationale

To enable for virtualization technologies and capabilities the SDT added, "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code" as an option in Attachment 1 Section 5 Part 5.2.1.

The final bullet of Attachment 1 Section 5 Part 5.2.1 was preceded with the language "Review of" to make the requirement for other methods parallel to the five options listed above it.

Attachment 1 Section 5 Part 5.3

Rationale

To enable for virtualization technologies and capabilities the SDT added, "or VCA" in Attachment 1 Section 5 Parts 5.3.1.

To ensure SCI supporting a low impact BCS are afforded equal protections from malicious code when using Removable Media, the SDT added "SCI that supports a low impact BCS" to the low impact BCS in Attachment 1 Section 5 Parts 5.3.1 & 5.3.2.

Attachment 2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to shorten applicability statements within the body of CIP standards with "BCS" as the defined acronym for "BES Cyber System". Additional changes were to align the Attachment 2 Measures with the modifications to the Attachment 1 requirement language.

Former Background Section from Reliability Standard CIP-003-8

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Technical Rational for Reliability Standard CIP-003-8

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-003-8 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media

- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an "electronic boundary" associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the "electronic boundary." This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an "electronic boundary," but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only "necessary" inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for "necessary" inbound and outbound electronic access controls may be documented within the Responsible Entity's cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

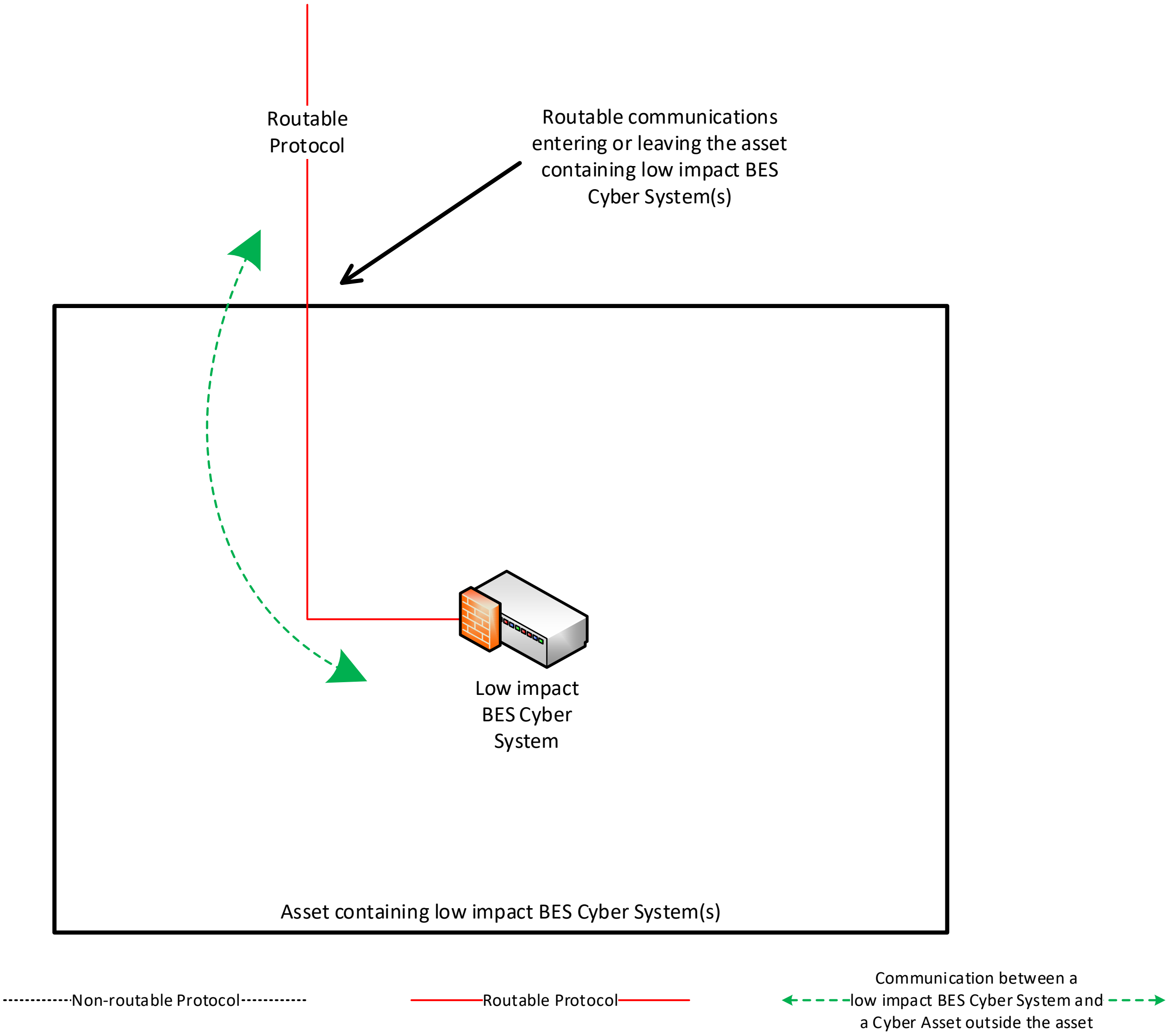
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

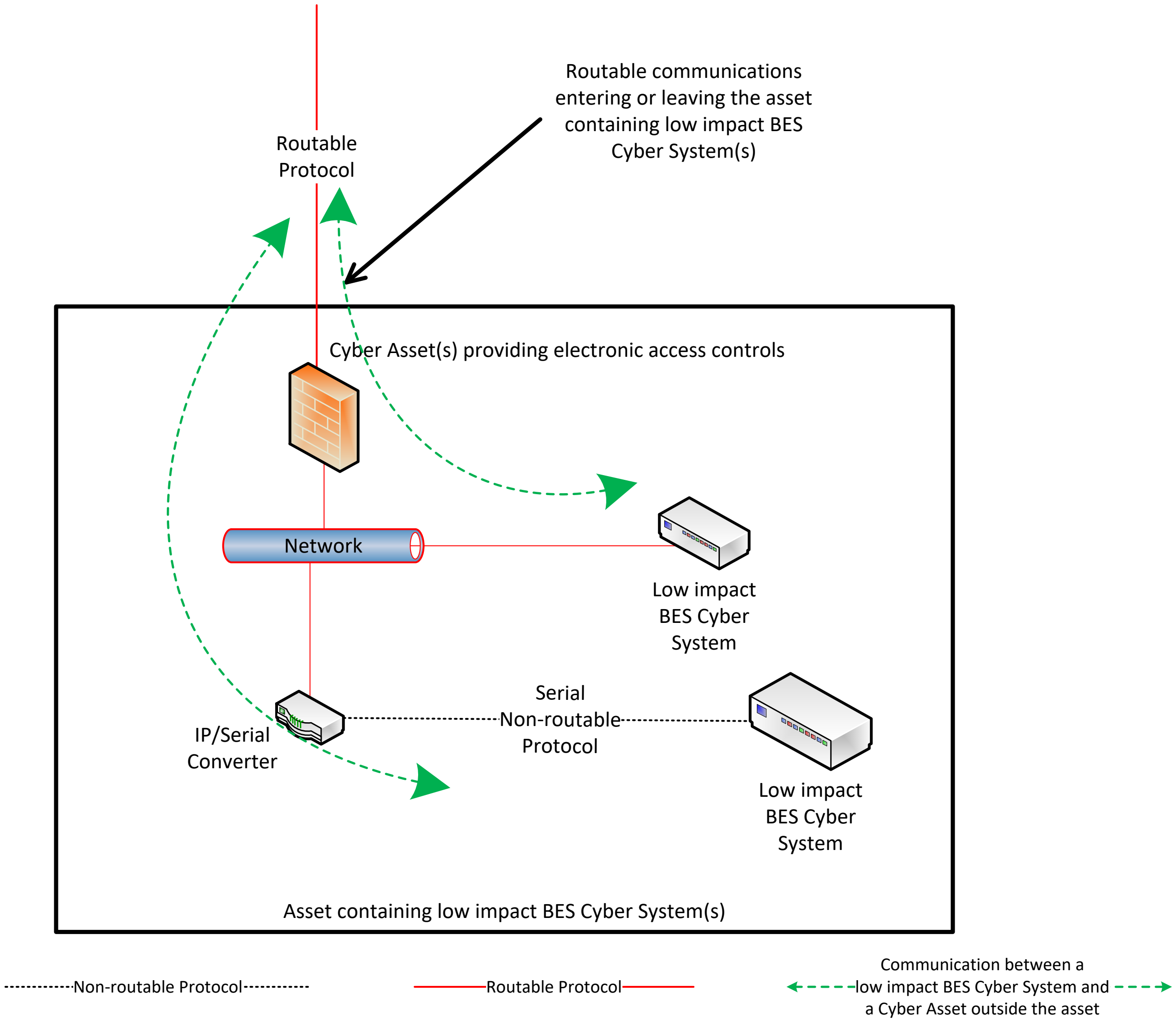
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

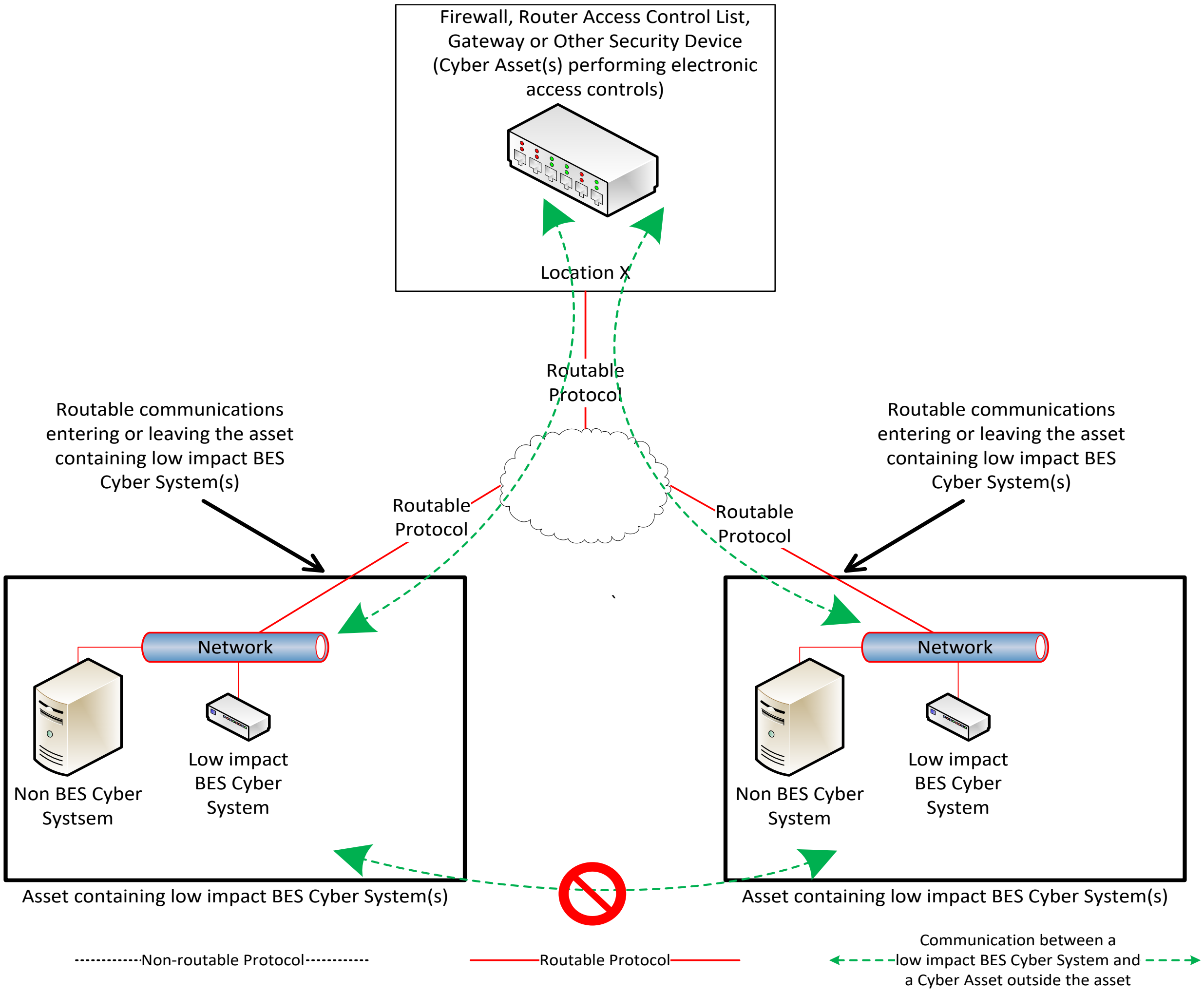
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

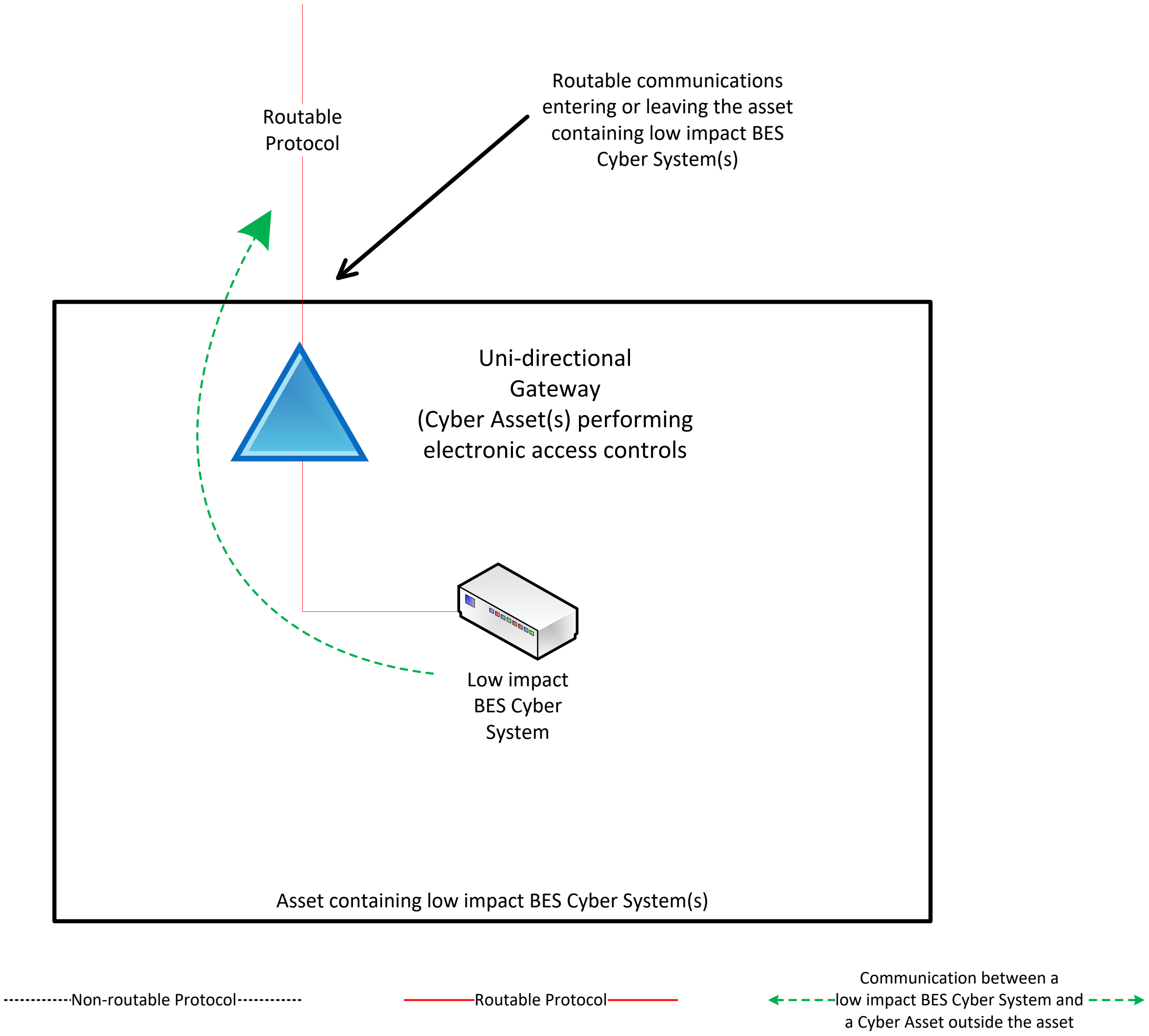
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at "Location X" to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

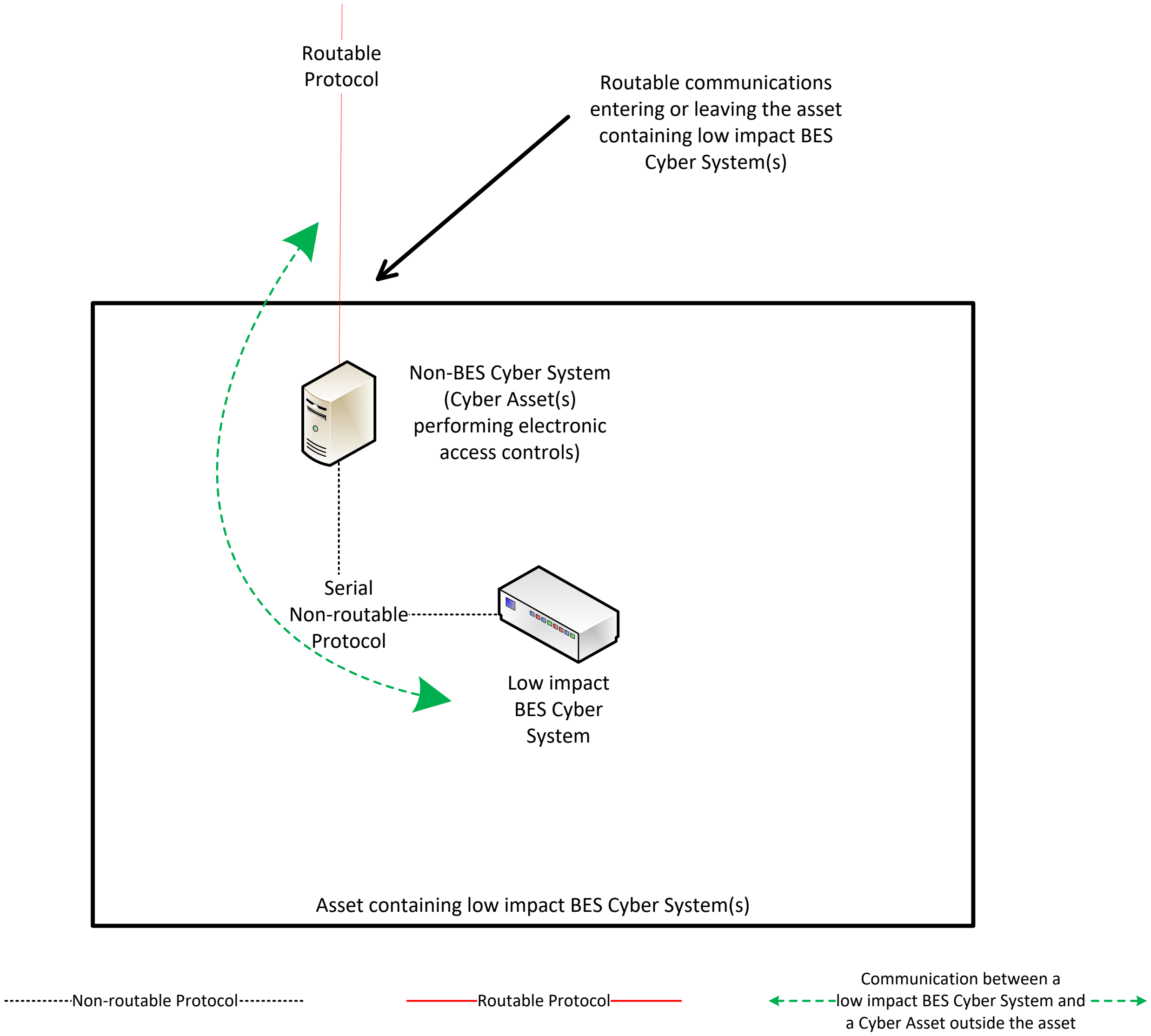
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a "one-way" (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

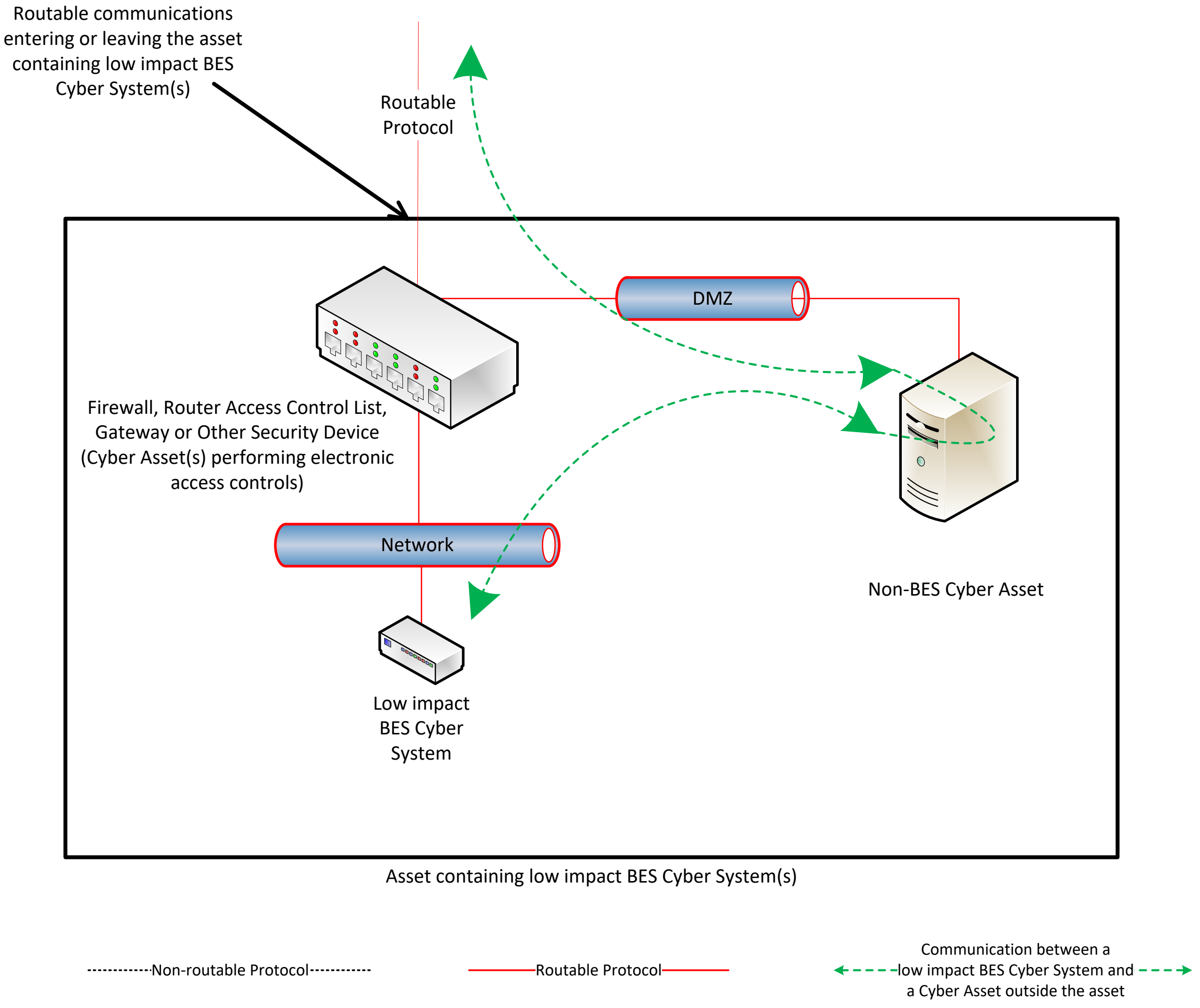
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

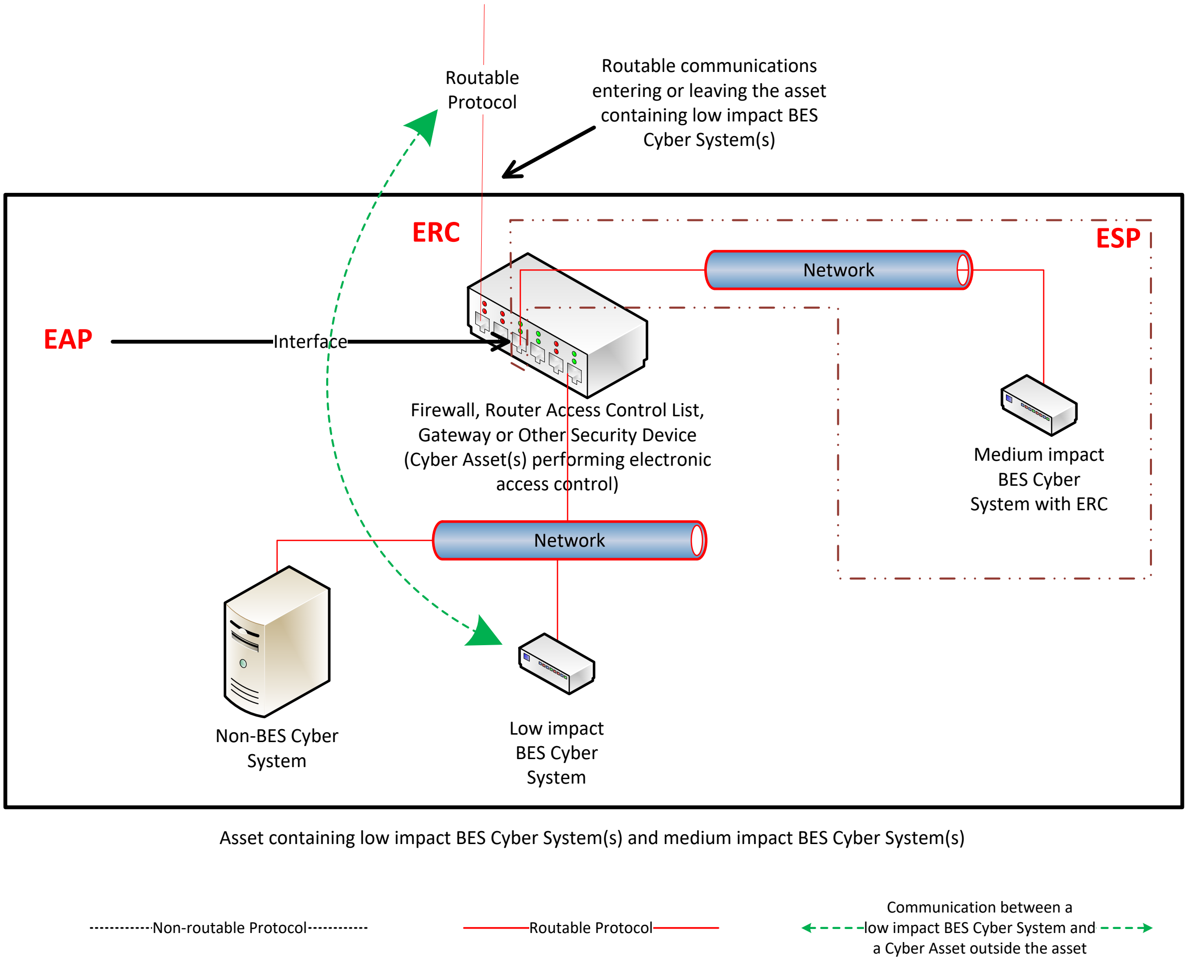
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.



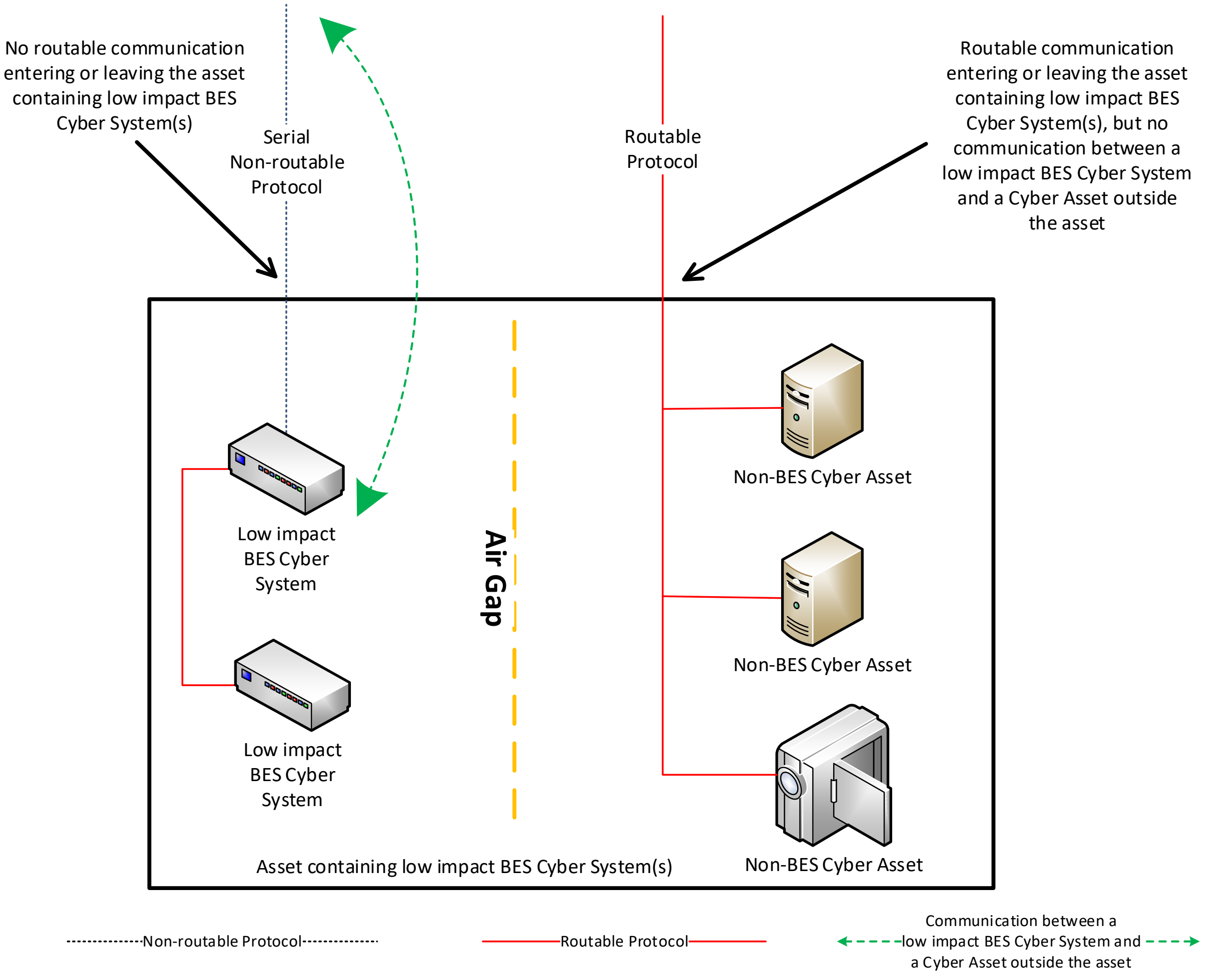
Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).

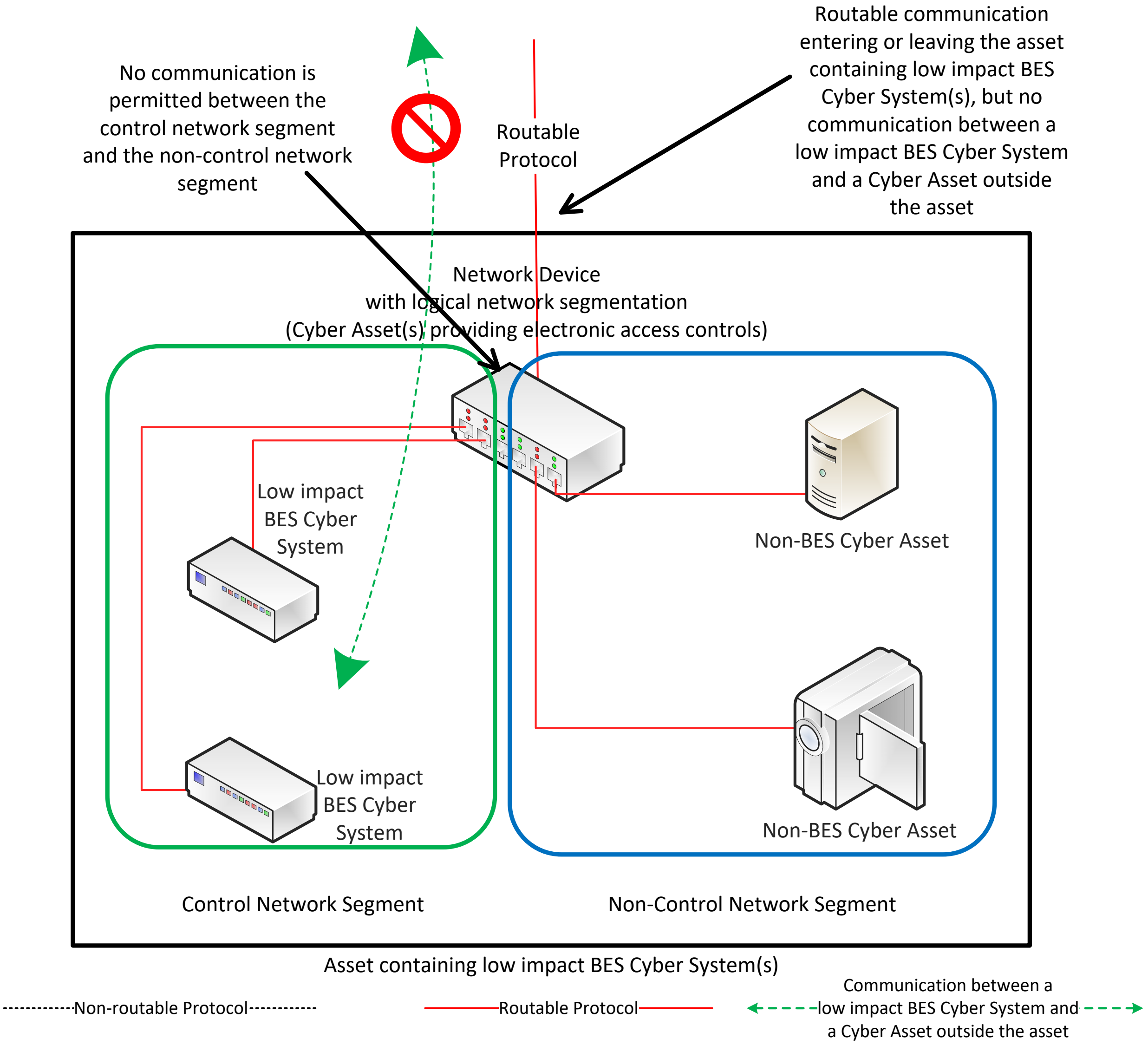
Section 1.



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

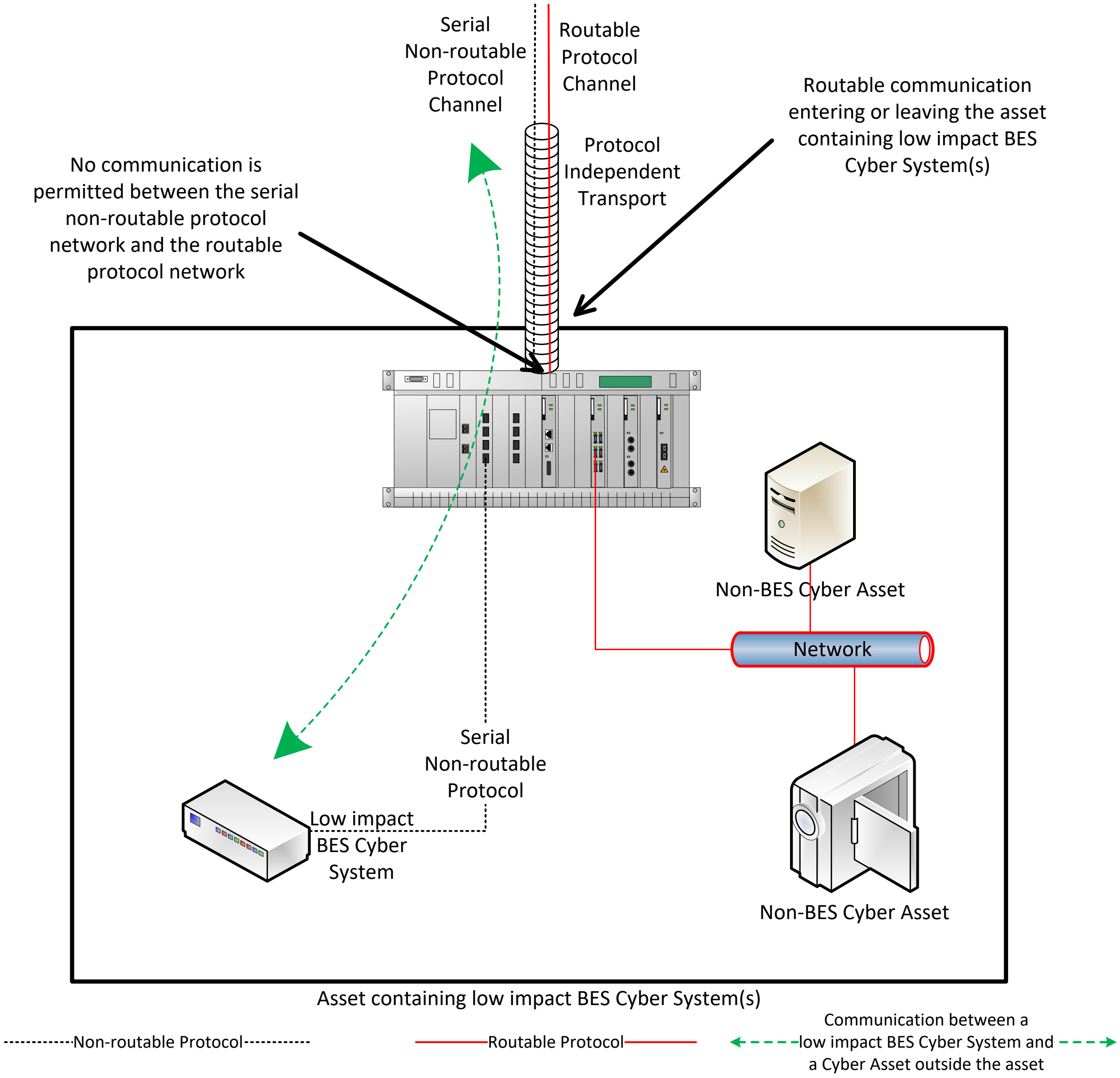
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity’s response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, “A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.” The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement

R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2.1: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.

---

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Section 5.2.2: The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-8

August 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-004-8

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-004-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the issues identified by the V5TAG was virtualization. The V5TAG Transfer document states, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." Document for reference when reading the technical rationale that follows.

Requirement R1-R6

General Considerations

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-004-8 to align personnel and training requirements with the virtualization changes.

To enable CIP-004-8 for virtualization, the SDT added "Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part" within the Applicable Systems column of each of the Parts for Requirement R1 – Requirement R6.

Additionally, where the term BES Cyber System (BCS) was used in the requirement language, it is replaced with "Applicable Systems" to align the requirement language of each Requirement Part with the updated applicability for each Requirement Part.

Requirement R3 Part 3.5

Summary of Changes:

A CIP Exceptional Circumstance was added as an exception to “Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 through 3.4 within the last seven years” such that individuals granted authorized electronic access and authorized unescorted physical access have undergone the personnel risk assessment processes.

Change Rationale:

The SDT determined Responsible Entities cannot require personnel risk assessments for first responders prior to granting them authorized unescorted physical access during certain conditions that qualify as CIP Exceptional Circumstances.

Former Background Section from Reliability Standard CIP-004-7

This section contains a "cut and paste" from the **Background** section of the Standard. It was retired and removed, and is provided as-is to preserve any historical references. No modifications have been made.

Background

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

The following conventions are used in the “Applicable Systems” column as described. High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

General Considerations for Requirement R1

None

Rationale for Requirement R1

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table Requirement R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets (TCA) and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, TCA and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3

General Considerations for Requirement R3

None

Rationale for Requirement R3

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new personnel risk assessment (PRA). Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4

General Considerations for Requirement R4

None

Rationale for Requirement R4

Authorization for electronic and unescorted physical access must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5

General Considerations for Requirement R5

None

Rationale for Requirement R5

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5 Part 5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement R5 Part 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the Bulk Electric System. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Requirement R6

General Considerations for Requirement R6

None

Rationale for Requirement R6

Requirement R6 requires Responsible Entities to implement a BES Cyber System Information (BCSI) access management program to ensure that provisioned access to BCSI is authorized, verified, and promptly revoked. Authorization ensures only individuals who have a need are authorized for provisioned access to BCSI. Prompt revocation of terminated individuals' ability to access BCSI helps prevent inappropriate disclosure or use of BCSI. Periodic verification ensures that what is currently provisioned is authorized and still required, and allows the Responsible Entity the opportunity to correct any errors in provisioning.

The change to "provisioned access" instead of "designated storage locations" enables the use of third-party solutions (e.g., cloud services) for BCSI. The concept of "designated storage locations" is too prescriptive and limiting for entities that want to implement file-level rights and permissions (i.e., policy based credentials or encryption keys that follow the file and the provisioned individual), which provide BCSI access controls regardless of storage location. The concept of provisioned access provides the needed flexibility for entities to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

According to Requirement R6, Part 6.1, the Responsible Entity must authorize individuals to be given provisioned access to BCSI. First, the Responsible Entity determines who needs the ability to obtain and use BCSI for performing legitimate work functions. Next, a person empowered by the Responsible Entity to do so authorizes—gives permission or approval for—those individuals to be given provisioned access to BCSI. Only then would the Responsible Entity provision access to BCSI as authorized.

Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI.

For BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet. For BCSI in electronic format, electronic access is provisioned to an electronic system or its contents, or to individual files. Provisioned physical access alone to a physical location housing hardware that contains electronic BCSI is not considered to be provisioned access to the electronic BCSI. Take, for instance, storing BCSI with a cloud service provider. In this case, the cloud service provider's personnel with physical access to the data center is not, by itself, considered provisioned access to the electronic BCSI stored on servers in that data center, as the personnel would also need to be provisioned electronic access to the servers or system. In scenarios like this, the Responsible Entity should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011-X. The subparts in Requirement R6, Part 6.1 were written to reinforce this concept and clarify access management requirements.

The periodic verification required by Requirement R6 Part 6.2 is to ensure that only authorized individuals have been provisioned access to BCSI and that what is provisioned is what each individual currently needs to perform work functions. For example, by performing the verification, the Responsible Entity might identify individuals who have changed jobs and no longer have a need for provisioned access to BCSI, and would therefore revoke provisioned access.

For Requirement R6 Part 6.3, removal of an individual's ability to use provisioned access to BCSI is considered to mean a process with the result that electronic access to electronic BCSI and physical access to physical BCSI is no longer possible from that point in time onwards using the means the individual had been given to obtain and use BCSI in those circumstances. Either what was specifically provisioned to give an individual access to BCSI (e.g., keys, local user or database accounts and associated privileges, etc.) is taken away, deleted, disabled, revoked, etc. (also known as "deprovisioning"), or some primary access is removed which prevents the individual from using the specifically provisioned means. Requirement R6 Part 6.3 acknowledges that where removing unescorted physical access and Interactive Remote Access, such as is required in Requirement R5 Part 5.1, prevents any further access to BCSI by the individual after termination, then this would constitute removal of an individual's ability to use provisioned access to BCSI. Access can only be revoked or removed where access has been provisioned. The intent is not to have to retrieve individual pieces of BCSI (e.g., documents) that might be in someone's possession (although you should if you can, but the individual cannot un-see what they have already seen).

Where no specific mechanisms are available or feasible for provisioning access to BCSI, these requirements are not applicable. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BCSI, such as when the individual is handed a piece of paper during a meeting or sees a whiteboard in a conference room. Likewise, these requirements are not applicable where provisioned electronic or physical access is not specifically intended to provide an individual the means to obtain and use BCSI. There will likely be no specific provisioning of access to BCSI on workstations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BCSI is only temporarily or incidentally located or stored there. Another example is the provisioning of access to a substation, the intent of which is to enable an individual to gain access to the substation to perform substation-related work tasks, not to access BCSI that may be located there. However, BCSI in these locations and situations still needs to be protected against unauthorized access per the Responsible Entity's information protection program as required by CIP-011-X.

The change to “provisioned access” to BCSI is backwards compatible with the previous “designated storage locations” concept. Entities have likely designated only those storage locations to which access can be provisioned, rather than any location where BCSI might be found. Both concepts intend to exclude those locations where BCSI is temporarily stored, as explained in the previous paragraph. Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of information. The removal of the term “designated storage location” does not preclude an entity from defining storage locations for the entity’s access management program for authorization, verification, and revocation of access to BCSI.

Technical Rationale for Reliability Standard CIP-004-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

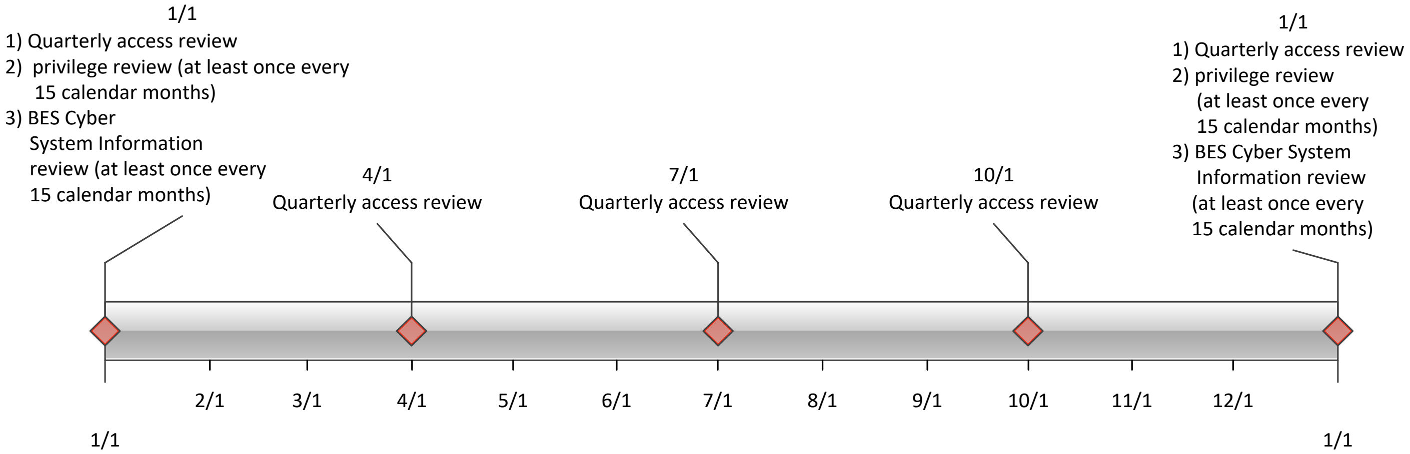
A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.



Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing “immediate” revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security – BES Cyber System Logical Isolation

Technical Rationale and Justification for Reliability Standard CIP-005-8

August 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-005-8

Introduction

This document is the technical rationale and justification for Reliability Standard CIP-005. It includes the rationale for changes in the current proposed version (CIP-005-8) as well as previous versions of the standard. The intent of this document is to provide stakeholders and the ERO Enterprise with an understanding of the revisions and the technical concepts of the Reliability Standard as well as the rationale for such revisions, both the currently proposed and historical revisions from previous versions and SDTs.

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition Advisory Group (V5TAG), which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005-8 and the definitions of Cyber Asset and Electronic Access Point (EAP) that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

Summary

The Project 2016-02 Standard Drafting Team (SDT) proposal accommodates for increasing use of virtualization and other technology innovation. The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards, but also to better position the CIP standards to be applicable to additional future technological innovation while, to the extent possible, maintaining backwards compatibility.

CIP-005-8 remains a standard concerned with controlling communications to and from BES Cyber Systems (BCS) by establishing an Electronic Security Perimeter (ESP) with increased security controls for Interactive Remote Access (IRA) and vendor remote access. However, virtualization is enabling models for network security, such as "Zero Trust", that are not network perimeter based. Therefore, in CIP-005-8 the ESP focuses on being a security model rather than a network topology-based perimeter as the only option. Securing the communications to and from BCS is the security objective, but the standard no longer prescribes "where", as in where on a network, the controls must be implemented. Innovations such as Zero Trust models are moving access control from network borders to a session level orientation and eliminating the implicit trust within a local network. Network perimeter-based ESP and EAP implementations remain a valid option and are one method for allowing only necessary communications to the Cyber

Systems within the ESP. The ESP definition now has a two “flavors”, the original ESP definition unchanged as the first “flavor”, and the new boundary based model that enables zero-trust as the second.

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in “CIP Definitions and Exemptions Technical Rationale” document for reference when reading the technical rationale that follows.

Requirement R1 General Considerations

ESP Redefined

Network border-based ESPs and EAPs remain a valid option for controlling the communications to and from BCS. However, virtualization technologies and models such as Zero Trust present equally effective methods that are not network border-based solutions. A Zero Trust model can implement more granular controls throughout a network on a per-access or per-session level.

Shared infrastructure and “Mixed Trust” Risks

For virtualized environments where SCI is used, a risk of side channel attacks exists. Virtualization allows disparate workloads of what could be differing impact to execute on the same CPUs and share the same memory (i.e. RAM). In this case the lower impact systems would become high water marked with the higher impact system through the PCA definition. This would in turn affect what requires protection by any associated ESPs . The risks associated with this scenario is mitigated in CIP-005-8 by either:

- Declaring the VCAs that share CPU or memory or are within the same ESP with a BCS as associated PCAs which will require they meet the security requirements (high water marking) that include ‘associated PCAs’; or
- Configuring the virtualization infrastructure to place VCAs of differing impact or trust levels into differing CPU and memory pools and configuring affinity controls to these pools such that hypervisors do not allow workloads in these differing pools to simultaneously exist or execute on the same hypervisor.

Assets with Multiple Classifications (PCA, EACMS, Intermediate System, SCI, etc.)

The definitions created to categorize Cyber Assets have historically included overlap. The definition of PCA was revised to include VCAs that share CPU or memory with a BCS. Additional definitions such as SCI and VCA will add to the possibility of additional instances of assets or systems meeting multiple definitions, such as SCI that are also EACMS.

These definitions are used in both the Applicable Systems column as well as within the requirement language. The fact that one asset or system may meet multiple definitions and therefor have multiple classifications does not pose a significant challenge as long as the Responsible Entity ensures that all requirements that pertain to ANY of the classifications are applied. In other words, if an asset or system meets both the SCI and the EACMS definition, requirements that apply to either categorization are applicable.

Firewall/Router on a Stick

A “firewall on a stick” or “router on a stick” is a reference to a networking design scenario by which a firewall or router has one single physical connection to a switch, but has access to multiple networks and broadcast domains by utilizing logical interfaces in combination with VLANs (Virtual Local Area Networks).

Devices on different VLANs are not able to communicate by default, so the primary purpose of this design is to allow for inter-VLAN routing enabling communication between devices which reside on different VLANs by way of the firewall or router.

As all traffic between these VLANs passes through the firewall or router it is uniquely positioned to restrict access and log traffic flows between devices on different VLANs facilitating compliance and the enforcement of security requirements.

This design allows an entity additional flexibility with respect to the creation of multiple Electronic Security Perimeters while minimizing the cost and number of physical networking devices required to provide proper levels of protection and isolation to each of the created Electronic Security Perimeters.

An entity may select this design to enable further isolation of distinct applications and systems from each other based on the assessed risk that they pose to the BES or to enhance their ability to control access to these systems.

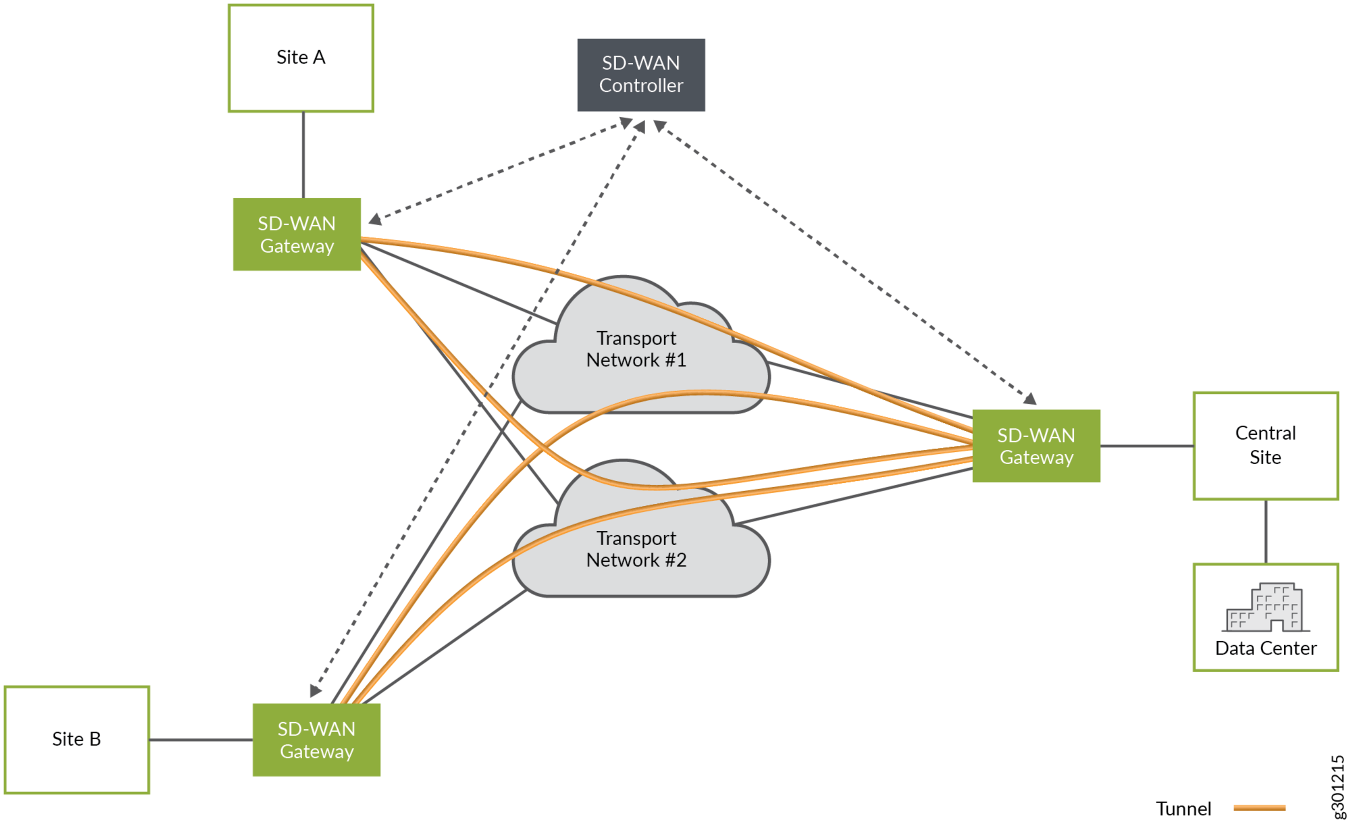
Careful attention should be given to the isolation and access control of management interfaces that support this design as they have the potential to impact multiple Electronic Security Perimeters.

SDWAN

Software-Defined Wide Area Networks (SDWANs) are comprised of an underlay network and an overlay network.

The underlay network is what we traditionally refer to as our Wide Area Networks and is constructed with various telecommunications provider circuits and technologies, including Serial, MPLS, LTE, Cable Modem, DSL, etc.

The overlay network is a virtual network layer created upon the underlay network, generally via encrypted tunnels or other similar mechanisms. An overlay network may utilize one or more underlay networks via load balancing or network policies. The policies governing the overlay network may dictate parameters such as what traffic is permitted, what underlay to utilize based on the application type, what should be utilized as the primary path, and various other parameters.



^^^ Inspiration for Matt, image sourced from Juniper Networks ^^^

SDWAN enables the construction of secured and isolated network paths with enhanced management and monitoring capabilities in addition to enabling additional services to and from the SDWAN such as VPN connectivity, firewall services, traffic inspection, and shared gateways.

This technology provides an increased level of control over Wide Area Networks while enhancing visibility, security, and redundancy, all while offering the potential to reduce the costs associated with providing connectivity between an entity's locations and assets.

VXLAN

VXLAN is similar in concept to SDWAN in that it is a form of a Software Defined Network, but in the case of VXLAN the focus is on networks within the Datacenter as opposed to SDWAN which focuses on networks between Datacenters and other facilities.

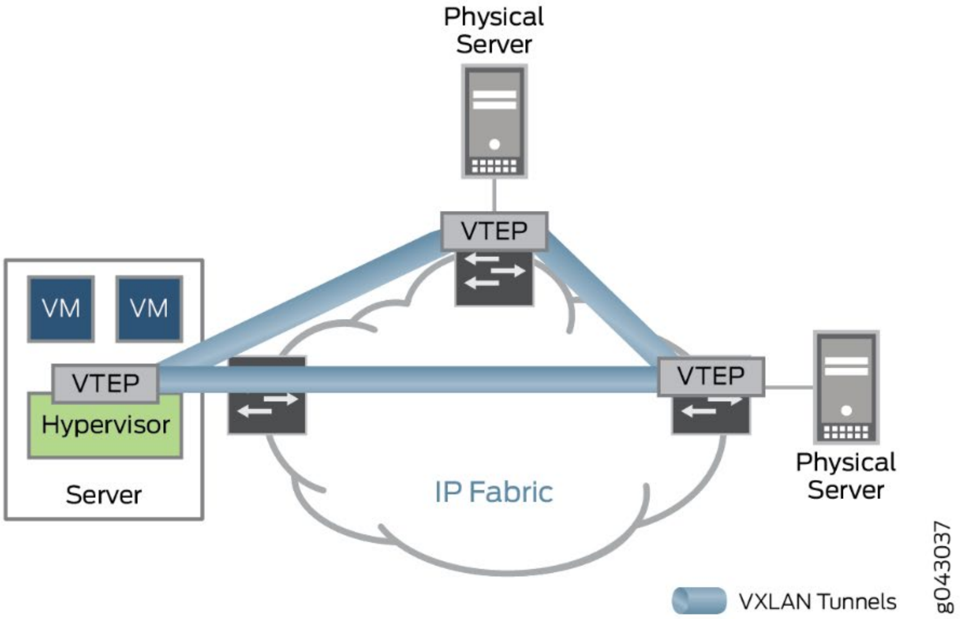
VLXLAN also utilizes the underlay and overlay terminology that we are familiar with given our review of SDWAN. The primary distinction is that VXLAN itself is the name of the overlay protocol utilized in this design and is the most common protocol used for overlay networks within a Datacenter.

The goal of VXLAN is to enhance the ability to segment network resources while also easing the burden of managing, automating, and orchestrating this segmentation by creating a virtual network that is agnostic of the physical network components supporting it.

The VXLAN protocol encapsulates Layer 2 Ethernet frames within Layer 3 UDP packets between devices comprising the design and allows for upwards of 16 million network segments to be created versus the traditional limit of 4094

VLANs. These network segments are identified with a VNI (VXLAN Network Identifier) which is synonymous to a VLAN ID.

The components of the design that are capable of encapsulating and de-encapsulating the VXLAN protocol are referred to as VTEPs (VXLAN Tunnel Endpoints) and are commonly network switches or virtual machine hypervisors. Physical devices and servers rely on switches to act as their VTEP whereas a virtual machine, hosted on VMWare ESX in this example, relies on the hypervisor as its' VTEP.



^^^ Inspiration for Matt, image sourced from Juniper Networks ^^^

VXLAN facilitates increasing the level of network segmentation within and between an entities Datacenters, while also enhancing their ability to automate and orchestrate the deployment of network resources. With this increased network segmentation an entity is granted more granular control over the flow of traffic and is given more opportunities to inspect that traffic to ensure appropriate levels of access control and protection.

Requirement R1

Rationale

Requirement R1 requires implementation of an ESP for BCS permitting only necessary communication through the ESP. However, there are other network security models available (such as zero trust) that can accomplish this security objective by controlling communications end-to-end at a more granular level than a network perimeter-based model. The definitions (ESP and EAP) and the changes to R1 allow entities the flexibility to implement different models that meet the security objective, or retain their current perimeter-based implementation.

Requirement R1 Part 1.1:

Rationale

This Requirement Part requires all high and medium impact BCS and their associated PCAs be protected by an ESP. In recognition of non-perimeter based models, the language changed from “shall reside within” to “must be protected by”. Note, a PCA can now be defined by two different attributes of what they share with a BCS – not only network location, but also the sharing of CPU and memory from the underlying hypervisor(s) for VCAs. In the instance that a VCA becomes an 'associated PCA' from its sharing of CPU or memory with a high or medium impact BCS, that associated PCA must also be protected by an ESP.

Note that this Requirement Part applies to all high and medium impact BCS without regard to external connectivity from the local network to other networks. This allows for the identification of PCAs and the scope of TCA connectivity even on isolated networks.

Requirement R1 Part 1.2:

Rationale

This Requirement Part changed to a security objective, rather than prescribing ERC must be controlled at an EAP. Virtualization technologies introduce additional methods to isolate systems. This requirement part no longer prescribes one method of controlling communications to Applicable Systems, and opens it up for alternative solutions.

This allows for other models such as zero trust architectures. Such models are not based on controlling communications at a Cyber Asset interface located on a network boundary. Communications can be authorized by software defined policy enforcement points throughout the infrastructure. In this model, network security is less topology-based and more policy-based (configurations and settings) and can be used to granularly protect communication at an individual system or even process or resource level.

While pure zero-trust architectures are an emerging model, the objective-based requirement also allows for hybrid models of various combinations of network border-based and zero trust architectures. As technology changes, this requirement and broadened ESP definition are flexible in how the objective is met.

The core security objective, of permitting only needed communications and denying all others by no longer prescribing this must be implemented at a Cyber Asset interface on a network border (an EAP), is retained. The intent of this Requirement Part is to control the 'reachability' of the Applicable Systems; filtering network communications *before* they reach the Applicable Systems and their OS, not as part of it. This is not to discourage the use of integrated host-based firewalls to further filter network traffic to a host.

Time-sensitive communications between Protection Systems (i.e., digital relays) that use routable communication protocols is excluded. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by inserting an ESP and its controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles (sub-second response times) to protect BES assets. The SDT intent is a Responsible Entity using this technology is not expected to implement the electronic access controls in a situation where it would prohibit the proper function in the proper timeframe.

Requirement R1 Part 1.3:

Rationale

The purpose of this new Requirement Part is to permit only needed communications to and from the Management Interfaces, denying all other communications, of the systems that are providing protection of BCS; namely SCI that is supporting an Applicable System from Part 1.1 (SCI isolates systems of different impact levels from each other) and EACMS that are enforcing an ESP (This Requirement Part only applies to SCI and EACMS enforcing an ESP, and not to the BCS itself). These are vital controls performing the isolation/segmentation between systems of differing impact levels, and warrant protection of the Management Interface that could be used to compromise them.

For the EACMS portion, a firewall that is enforcing an ESP, as well as a network switch configured with VLANs to isolate and segment traffic are intended to be included and have their Management Interfaces protected.

The 'per system capability' is included in this Part in recognition that some Management Interfaces, such as "ILO" interfaces, may do inbound but not outbound traffic controls.

Requirement R1 Part 1.4:

Rationale

The SDT included "SCI supporting an Applicable System in this Part" to the scope of the requirement part to ensure that controls regarding Dial-up Connectivity are also applicable to VCAs and SCI; and 'technical feasibility' has been replaced with the 'per system capability'.

Additionally, in order to maintain a decipherable Applicable Systems column the SDT replaced the scoping phrase "with Dial-Up Connectivity" from the Applicable Systems column, with a reference to "if any" in the Requirement Language.

Requirement R1 Part 1.5:

Rationale

Known or suspected malicious communication detection is specific to Internet Protocol (IP) based traffic that enters or leaves the required ESP. Products available to implement this malicious communication detection are usually based on IP traffic (as defined in RFC 791 and upon which TCP and UDP reside). Requirement applicability was changed to BCS instead of EAPs; lifting it to an objective level and keeping it from being a prescriptive 'where' that forces certain architecture.

Requirement R1 Part 1.6:

Rationale

Requirement R1 Part 1.6 was written to address the issue of "Super ESPs" with high or medium impact BCS at Control Centers that extend a single ESP beyond one PSP. This often applies to virtualized Control Center environments that implement network adjacency to allow workloads to automatically move from one physical location to another to increase BCS resiliency between primary and backup Control Centers.

The security objective is to protect the confidentiality and integrity of the data traversing communication links used to span a single ESP between multiple PSPs. This is especially important when portions of the transport are not within the Registered Entity's control. Many encryption methods (such as IPSec and TLS) can fulfil this objective, however some encryption methods fall short of providing both confidentiality and integrity controls.

This Requirement Part works in conjunction with the new 4.2.3.3 exemption in the CIP standards that exempts the Cyber Systems associated with such communication links since the data is required to be protected per this requirement. Also, the former CIP-006-6, Requirement R1, Part 1.10 has been removed and incorporated into this new 1.6 requirement part; consolidating the protections of an ESP and its components that extend outside of a PSP within one standard.

Communications equipment associated with communications links (e.g., equipment belonging to carriers) is exempted from the CIP standards with the 4.2.3.2 exemption, however that only applies to equipment between discrete ESPs. However, in this extended ESP situation where a single ESP spans multiple sites or PSPs, that exemption does not apply and the potential exists for data to traverse a connection that uses third-party communications equipment that is unprotected inside an ESP; hence the need to enforce confidentiality and integrity controls (such as encryption) on the data that traverses PSPs while within the same ESP to isolate any protected data from access through the communications equipment.

This consolidation also incorporates cabling and non-programmable communication components that are not PSP-protected, intending to protect data moving across the state as well as data traversing cabling that crosses the hall outside of the PSP. Note: the language specifically exempts the data that falls under CIP-012 Requirements in order to avoid the potential for double jeopardy as well as the time-sensitive protection or control functions as described in CIP-005-8 Requirement R1 Part 1.1 above.

Requirement R2:

General Considerations for Requirement R2.

External Routable Connectivity (ERC) and Interactive Remote Access (IRA)

The ERC and IRA definitions have been updated in order to:

1. Incorporate new models such as Zero Trust where a security perimeter is not necessarily a network perimeter and ESP's become very granular based on policies that can be established at "people to resource" levels rather than IP address levels.
2. Recognize those Cyber Systems that are of an increased risk due to their "reachability" via ERC and that have IRA available to them even if they are serial-only, non-routable devices.
3. Continue to limit scope of Requirement Parts to BCS with ERC and not those that have connectivity such as non-routable serial leased circuits.

The V5TAG transfer document in the SDT's scope include the issue of a BES Cyber Asset (BCA) that only uses non-routable protocols over a serial port. These BCAs are not connected to a network with a routable protocol themselves and therefore can be considered to not be within an ESP and thus not have ERC. However, these BCAs can have interactive user access using those serial connections. The SDT's intent is to clarify that IRA can occur to a device with only a serial, non-routable connection through IP-to-serial conversions and be subject to CIP-005-8 Requirement R2. For example, the intent is to clearly cover situations where a serial-only, non-routable BCA, such as a digital relay in a substation, has its serial communication from a 'console port' converted to IP or other routable protocols thus allowing IRA from users outside the substation to use a routable protocol to interact with the serial device and to require the CIP-005-8 Requirement R2 protection for that IRA.

The SDT removed the requirement-style language "The Intermediate System must not be located inside the Electronic Security Perimeter" from the Intermediate System definition in favor of a clarified objective in CIP-005-8 Requirement R2 that all IRA must be *through* an Intermediate System. Requirement R2 Part 2.6 was added to objectively address the location of the Intermediate System.

See the "*CIP Definitions and Exemptions Technical Rationale*" document for further explanation of the changes to the R2 related definitions.

Requirement R2 Part 2.1:

Rationale

Applicable Systems was updated to include SCI to ensure the same safeguards for remote access methods exist for SCI supporting an Applicable System within the Part as they do for the high and medium impact BCS and associated PCA hosted on that SCI. Backwards compatibility is retained for entities that do not use SCI.

The requirement language was simplified, and definitions for IRA and Intermediate System have been updated. Please note that the definition of IRA was changed to include serial communications that are converted to/from routable protocols by the Responsible Entity. This change maintains backwards compatibility except where serial connectivity and routable protocol conversion is being used for IRA.

Requirement R2 Part 2.2:

Rationale

The "Applicable Systems" scope was changed to "Intermediate Systems used to access Applicable Systems of Part 2.1". This clarifies this requirement is associated with the IRA communications between an Intermediate System and the remote clients, as opposed to between the Intermediate System and the BCS. This is important so that it does not require encryption through the ESP to the BCS which would hinder monitoring and inspection.

The requirement was changed from a specific technical-based requirement for encryption to an objective-based requirement to protect confidentiality and integrity of the IRA session between the Intermediate System and the remote client (with encryption as a primary example). The proposed language accounts for the possibility that other equally effective methods could be developed and deployed. This objective also keeps methods from being used that are merely obfuscation methods (XOR, ROT13, etc.) or deprecated encryption methods (DES with 56-bit keys) that no longer meet the objective to protect the confidentiality and integrity of the IRA session.

The changed requirement is backwards compatible except where deprecated encryption methods are in use.

Requirement R2 Part 2.3:

Rationale

The Applicable Systems was changed to "Intermediate Systems used to access Applicable Systems of Part 2.1". This clarifies this requirement is associated with the Intermediate System itself, and where the requirement for multifactor authentication should be applied (multi-factor authentication to the Intermediate System).

Requirement R2 Part 2.4 – 2.5:

Rationale

The Applicable Systems section of this requirement was updated to include SCI for instances where vendor remote access is allowed to the SCI. The Applicable Systems were also modified such that only those with vendor remote access are in scope and thus need to have one or more methods for CIP-005-8 Requirement R2 Parts 2.4 and 2.5.

The requirements themselves have not changed.

Requirement R2 Part 2.6:

Rationale

This is a new requirement that applies to Intermediate Systems. The intent of this new requirement is to further protect the BCS from the Intermediate System by reducing the attack surface between the two. Intermediate Systems have an externally accessible interface that may be used by external parties such as vendors or entity support staff using IRA across an Internet connection to support a remote site. Since Intermediate Systems by nature provide IRA from a less-trusted network and are accessible from yet-to-be authenticated users (in order to authenticate them), a degree of separation from the higher-trust systems they are protecting is necessary in case the Intermediate System is compromised. Previously, this risk was addressed within the glossary definition of Intermediate System ("…must not be located inside the ESP") instead of within an actual requirement. The SDT removed this from the definition and included a security objective in CIP-005-8 Requirement R2 Part 2.6 to require that routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.

It is important to note that a virtualized Intermediate System (VCA) hosted in such a way that it can share CPU and memory with a BCS will also meet the definition of PCA and become an 'associated PCA' of the BCS. CIP-005 R1.1 requires that PCA to be within an ESP, in conflict with this requirement. This is by design, and thus a VCA performing the function of an Intermediate System must not share CPU or memory with the BCS it is controlling access for. This is due to the access granted to the less trusted side of the Intermediate System and the risk is has for side-channel attacks to other VCAs sharing the same CPU and memory. Entities must therefore use affinity rules or some other means to keep Intermediate System VCAs from sharing the same CPU and memory as a BCS or its associated PCAs.

Requirement R3

Rationale

The Applicable Systems section of CIP-005-8 Requirement R3 was updated to include SCI to ensure the same safeguards for vendor-initiated remote connections exist for the applicable SCI. Backwards compatibility is retained for entities that do not currently use SCI.

Former Background Section from Reliability Standard CIP-005-7

This section contains a "cut and paste" from the **Background** section of the Standard. It was retired and removed, and is provided as-is to preserve any historical references. No modifications have been made.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BCS and require a minimum level of organizational, operational and procedural controls to mitigate risk to BCS.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BCS. For example, a single training program could meet the requirements for training personnel across multiple BCS.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.

- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

Technical Rationale for Reliability Standard CIP-005-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The ESP serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.

But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e. system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the “first line of defense within an Industry Control System (ICS) network environment”. The compromise of those devices that control access management could provide an outsider the “keys to the front door” of the ESP where BES Cyber Systems reside. An intruder holding the “keys to the front door” could use those “keys” to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability

Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[1].

NERC's final report on "*Cyber Security Supply Chain Risks"*, states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

---

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-005-6 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an “Associated Protected Cyber Asset” of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually ‘command and control’ hosts on the Internet, or compromised ‘jump hosts’ within the Responsible Entity’s other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT’s intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity’s address space. The SDT’s intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and ‘deny by default’ type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear ‘perimeter type’ security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions (“TFEs”) rather than increased security.

As for dial-up connectivity, the Standard Drafting Team’s intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple

redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.
But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Physical Security of BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-006-7

August 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-006-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-006-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-006-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-006-7 to shorten applicability statements within the body of CIP standards by replacing some terms with the defined acronym for that term:

"BCS" has replaced "BES Cyber System".

"ERC" has replaced "External Routable Connectivity".

"PSP" has replaced "Physical Security Perimeter".

"PACS" has replaced "Physical Access Control Systems".

Requirement R1

Rationale

The SDT made conforming changes to Applicable Systems for virtualization such that protections must be afforded to SCI for relevant Requirement Parts.

Applicable Systems:

Requirement R1 Part 1.1-1.9: the SDT added "SCI supporting an Applicable System in this Part.

Per System Capability vs Technical Feasibility:

Requirement R1 Part 1.3: The SDT chose to remove the reliance on a Technical Feasibility Exception in favor of the updated term "per system capability."

Consolidation:

Requirement R1 Part 1.10: The SDT deleted Requirement R1 Part 1.10 from CIP-006-7 because requirements to protect the data traversing communication links used to span a single ESP between PSPs is incorporated into CIP-005-8 Requirement R1 Part 1.6.

Requirement R2

Rationale

The SDT has include the CIP Exceptional Circumstances within the main R2 requirement text so that it applies to all requirement parts.

The SDT made conforming changes to Applicable Systems for virtualization such that protections must be afforded to SCI for relevant Requirement Parts.

Applicable Systems:

Requirement R2 Part 2.1-2.3: the SDT added "SCI supporting an Applicable System in this Part"

Former Background Section from Reliability Standard CIP-006-6

This section contains a "cut and paste" from the **Background** section of the Standard. It was retired and removed, and is provided as-is to preserve any historical references. No modifications have been made.

Background

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-006-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-006-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the PSP.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.

- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A logbook or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more PSPs, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System, but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an "an equally effective logical protection" in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity's BES Cyber Systems while not requiring controls to be implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the PSP to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the PSP. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a PSP (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any PSPs protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — System Security Management

Technical Rationale and Justification for Reliability Standard CIP-007-7

August 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-007-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-007-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-007-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale.pdf" for reference when reading the technical rationale that follows.

General Considerations

Requirement R1

General Considerations for Requirement R1

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To enable CIP-007-7 for virtualization, the SDT added "SCI supporting an Applicable System in this Part". This approach keeps the SCI applicability parallel to each existing variant of Applicable Systems in the same Requirement Part (i.e., Medium impact BCS vs. Medium impact BCS with External Routable Connectivity (ERC) vs. Medium impact BCS at Control Centers etc.)

Change Rationale Requirement R1:

The SDT has changed the name of the R1 table to "System Hardening" to more clearly reflect the security objective of the entries in the table which is to harden the applicable systems through limiting access to logical and physical ports, and to control where certain VCAs can instantiate through host affinity rules.

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical

Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCA.

Change Rationale Requirement R1 Part 1.1: Requirement R1 Part 1.1 requires "disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability". The SDT updated the Requirement Part language to be more objective concerning routable protocol network accessibility as opposed to "ports and services". Routable protocol access to a system is through services which open listening logical ports on a local network interface. R1.1 requires that any unneeded access over such be either disabled or prevented. "Accessibility" as used in R1.1 is at the logical, routable protocol network level and does not include physical access, logon to the physical console, code on TCA/RM, etc.

The objective is to reduce the attack surface on an applicable system preventing any unnecessary accessibility to the system using routable protocols. TCP/UDP port numbers are at times the best way to track this accessibility, at other times documenting enabled services is better. For example, hardening network accessibility in the physical underlay of SCI between hypervisors may be performed at a virtualization *services* level; turning off or disabling virtualization services that are not needed, rather than documenting the often proprietary and dynamic port numbers which may be of little value. However, in the overlay where an entity may be hosting a database server VCA on a virtual network, it may be easier to show that network accessibility is limited to two enabled ports and all others are disabled or blocked. The SDT has moved to this objective language to avoid attempts to prescribe the best way to document network accessibility in all the various scenarios and implementations. In addition, it is limited to routable protocol network accessibility such that non routable network communications (e.g., SAN over Fiber Channel) do not fall within scope of the Requirement Part.

The SDT added the clarifier "on each Applicable System" to indicate that the intent of this requirement is for an entity to perform the configuration actions on each Applicable System, hardening the system from its routable protocol network peers (e.g., east/west traffic within an ESP) rather than having a single method such as an EAP network firewall rule that would disable such accessibility for a group of Applicable Systems.

The SDT chose to remove the reliance on a Technical Feasibility Exception (TFE) in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE. The 'per system capability' also allows for devices that have no provision for disabling logical ports or services, such as some firmware-based devices with very limited configuration capabilities.

Note that the Measures language has been updated to aid backwards compatibility.

Change Rationale Requirement R1 Part 1.3:

Requirement R1 Part 1.3 is a new requirement intended to apply host affinity controls to SCI that supports the Applicable Systems listed. The risk associated with this SCI is such that it may host VCAs of different impact categorizations and requires additional hardening controls to mitigate the risk for side-channel attacks from VCAs of differing impacts sharing the same CPU and memory.

Note that the SCI definition covers only those portions of entity's virtualization infrastructure that support systems of differing impact levels. As VCAs that share the same CPU or memory with any part of the highest rated BCS are already PCAs (and thus share the same impact categorization), this requirement is only needed to cover instances where different impact categorizations are supported. This may occur when part of the same SCI supports different BCS and the entity does not wish to high watermark all the BCS together.

For example, this requirement would apply where the same SCI supports both a BCS with a high impact categorization on one part of a virtualization cluster, and a different BCS with a low impact categorization on a different part of the virtualization cluster. The proper use of host affinity controls would not require the BCS with the low impact categorization to be considered an “associated PCA” of the high (assuming the low impact BCS is also not in the ESP of the high impact BCS) as long as new controls for SCI are in place, such as affinity controls.

Requirement R2

Change Rationale Requirement R2:

The SDT chose to include the “SCI supporting an Applicable System in this Part” language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA(s) used in applicable BCS, EACMS, PACS or PCA.

The SDT made conforming changes where necessary with Requirement R2 to remove reliance on the Cyber Asset term, choosing to reference the Applicable Systems instead.

Additionally, the SDT chose to insert the word “cyber” as a clarifier to security patches for consistency with the term used in R2.1.

Backward Compatibility

CIP-007-7 Requirement R2 retains backward compatibility for entities that do not utilize SCI.

The SDT intends that entities take full advantage of their virtualization infrastructure in order to ease the overhead associated with patch management. While many of the entity’s existing processes will remain the same, (such as those associated with tracking the source of cyber security patches, evaluation of the applicability of available patches and mitigation plans for those applicable patches that cannot be installed) new or modified processes around the installation of patches can be used (for example, parent images, remediation VLANs, etc.).

Parent Images

One of the interesting nuances of virtualization is the concept of parent/child relationships.

Some VCAs utilize a “parent image” type methodology where the specific VCA software and operating system is merely a child instance of a parent image. In such cases, the application of cyber security patches to the parent image also applies the same changes to any children of that image. As there may be many child instances, the administrative overhead associated with patching of those instances can be greatly reduced.

Dormant Instances

There are times when VCAs are not being used and are idle. Physical instances of the assets are left up and running in order to receive applicable patches, software updates, configuration updates, etc.

Leveraging the built-in virtualization features allows idle resources to be reassigned to tasks at hand without incurring additional overhead of tracking which dormant virtual instances require patching. Dormant virtual instances are just files with the saved state of the VCA. Dormant instances are not VCAs themselves nor Applicable Systems until they become active instances again.

Where a dormant virtual instance is also the child instance of a parent image, the application of security patches to the parent image will also make the same changes automatically when needed to any out of date dormant child virtual instances when they are restarted.

In most cases, a dormant virtual child instance is made active again on a remediation type network where any missing security patches (compared to the parent image) are automatically applied before it is placed back into active service.

Saved Images

Similar to dormant child images, saved child images or snapshots may be also used as functional backups for CIP-009 purposes in order to provide fast restoration and better availability. If an active VCA becomes corrupted, a saved image can be made active where the application of any missing security patches (compared to the parent image) can be automatically applied, through remediation, before being placed back into active service.

Requirement R3

Change Rationale Requirement R3:

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA.

Requirement R4

Change Rationale Requirement R4:

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA.

Change Rationale Requirement R4 Part 4.1:

The SDT determined the entire structure of the "at the BCS level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)" language could be simplified to "per system capability" since the Applicable Systems column clarifies what systems are included.

Additionally, the SDT chose to insert the word "security" as a clarifier to which events are to be logged.

Change Rationale Requirement R4 Part 4.2:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the "Cyber Asset" term, as well as the ambiguity that would have existed if the term "BES Cyber System" were left in place while the Applicability Column included SCI.

Change Rationale Requirement R4 Part 4.3:

The SDT also chose to remove the reliance on a TFE from Part 4.3 in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

Requirement R5

Change Rationale Requirement R5:

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCAs.

Change Rationale Requirement R5 Parts 5.1, and 5.6 – 5.7:

The SDT chose to remove the reliance on TFE in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

Change Rationale Requirement R5 Part 5.4:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the "Cyber Asset" term, replacing it with a per "system" capability.

Change Rationale Requirement R5 Part 5.5:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the "Cyber Asset" term, replacing it with a reference to the Applicable Systems.

Former Background Section from Reliability Standard CIP-007-6

This section contains a "cut and paste" of the former Section 6. Background which has been retired and removed from the Standard. It is provided to preserve any historical references. No modifications have been made.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-007-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-007-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration

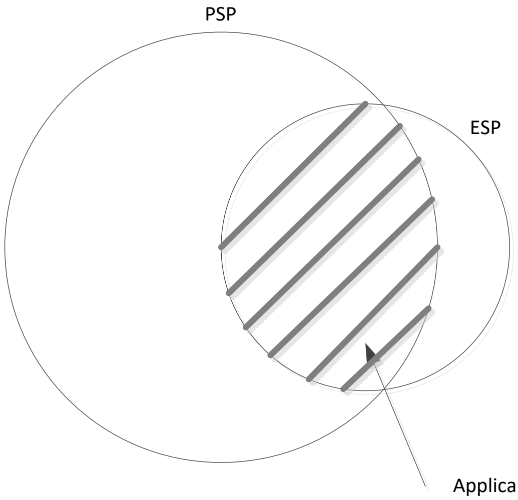
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a ‘defense in depth’ type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to “think before you plug anything into one of these systems” which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include “Nonprogrammable communication components located inside both a PSP and an ESP.” This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:

Location of Nonprogrammable Communication Components



Applicability of CIP-007-6 R1, Part 1.2 for Nonprogrammable Communication Components

Requirement R2:

The SDT’s intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an “install every security patch” requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.

- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security – Incident Reporting and Response Planning

Technical Rationale and Justification for Reliability Standard CIP-008-7

August 2022

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-008-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-008-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 – Requirement R4

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-008-6 to align incident reporting and response planning requirements with the virtualization changes and protections for Shared Cyber Infrastructure (SCI) by adding "SCI supporting an Applicable System in this Part" to each of the Parts in Applicable Systems for Requirement R1 – Requirement R4.

Requirement R4

Rationale

The Project 2016-02 SDT made updates to reflect the change from the National Cybersecurity and Communications integration Center (NCCIC) to its successor organization Cybersecurity & Infrastructure Security Agency (CISA), and deleted the historical footnote in favor of deference to the Requirement language, which already states "or their successors".

Former Background Section from Reliability Standard CIP-008-6

Section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:
Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

Medium Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

Technical Rationale for Reliability Standard CIP-008-6

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-6. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-008-6 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 19, 2018, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 848. In this Order FERC directed the North American Electric Reliability Corporation (NERC) to "develop and submit modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access and Control or Monitoring System (EACMS)." (Order 848, Paragraph 1)

In response to the directive in Order No. 848, the Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require Responsible Entities to implement methods augmenting the mandatory reporting of Cyber Security Incidents to include: "(1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report included specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT)." (Order 848, Paragraph 3)[1]

New and Modified Terms Used in NERC Reliability Standards

CIP-006-6 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms:

Cyber Security Incident

A malicious act or suspicious event that:

- *For a high or medium impact BES Cyber System, compromises, or attempts to compromise the, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or*
- *Disrupts, or attempts to disrupt, the operation of a BES Cyber System.*

In response to FERC Order 848, Paragraph 1, the SDT modified the Cyber Security Incident definition to include Electronic Access Control or Monitoring Systems (EACMS) associated with high or medium impact BES Cyber Systems, in response to the Order.

---

[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

The addition of high and medium impact BES Cyber Systems considers the potential unintended consequences with the use of the existing definition in CIP-003-7. It also provides clarity that only low impact BES Cyber Systems are included within the definition. ESP or EACMs that may be defined by an entity for low impact BES Cyber Systems are not part of the definition.

An attempt to disrupt the operation of a BES Cyber System is meant to include, among other things, a compromise of a single BES Cyber Asset within a BES Cyber System. For example, malware discovered on a BES Cyber Asset is an attempt to disrupt the operation of that BES Cyber System.

Reportable Cyber Security Incident
A Cyber Security Incident that compromised or disrupted:

- *A BES Cyber System that performs one or more reliability tasks of a functional entity;*
- *An Electronic Security Perimeter of a high or medium impact BES Cyber System; or*
- *An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber Systems.*

The Reportable Cyber Security Incident definition was modified to comply with FERC Order 848. In response to Paragraph 54 of the Order, the SDT modified the definition to include incidents that compromised or disrupted an ESP or an EACMS. The team also added the qualifying clause for "A BES Cyber System that performs one or more reliability tasks of a functional entity" to clarify what was compromised or disrupted, thus not extending the scope to Protected Cyber Assets (PCAs). In response to comments, the SDT left the entire definition of BES Cyber system in Reportable Cyber Security Incident to provide clarity.

It is also important to understand the relationship between the two definitions, the requirement language, and how they work in concert to classify events and conditions at varied levels of significance as the Registered Entity executes its process and applies its defined criteria to determine if reporting is required.

Electronic Access Control or Monitoring Systems (EACMS)
The drafting team spent significant time discussing this topic among its members, through industry outreach, and with FERC staff. The team believes by not specifically referencing the five functions in Order 848, we have reduced complexity and made compliance with the Standard achievable. The drafting team asserts that the five functions are equivalent to the current definition of EACMS in the NERC Glossary of Terms. If entities have questions about application of the EACMS definition, the drafting team advises entities to discuss those questions directly with NERC.

Requirements R1, R2, and R3

General Considerations for Requirement R1, Requirement R2, and Requirement R3

FERC Order 848, Paragraph 1, directs modifications to Reliability Standards to require reporting of incidents that compromise, or attempt to compromise a responsible entity's ESP or associated EACMS. The intent of the SDT was to minimize the changes within CIP-008 and address the required modifications. To do this, the SDT added "and their associated EACMS" to the "Applicable Systems" column for Requirements R1, R2, and R3.

To add clarity to "attempts to compromise," the drafting team created Part 1.2.1 to require entities to establish and document their process to include criteria to evaluate and define attempts to compromise. This requirement maps to Requirement 4 Part 4.2, which requires entities to use that entity-defined process for determining which incidents entities must report.

The use of the language describing Cyber Security Incident(s) as being "an attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the 'Applicable Systems'" column for the Part is meant to clarify which Cyber Assets are in scope for attempts to compromise reporting by entities. This language is used throughout the standard.

Moving Parts of Requirement R1 to Requirement R4

To minimize the changes to Requirement R1, the SDT created Requirement R4 and consolidated all the CIP-008-6 reporting requirements. The SDT deleted Requirement R1 Part 1.2 reporting requirements from CIP-008-5, and moved them to Requirement R4 for this purpose.

Inclusion of "Successor Organizations" throughout the Requirement Parts

The SDT recognizes that organizations are constantly evolving to meet emerging needs, and may re-organize or change their names over time. The ICS-CERT has completed its name change to the National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems. The E-ISAC previously re-branded its name and may again in the future. By following Requirement R4 references to E-ISAC and NCCIC with "or their successors" the SDT is ensuring that Requirement R4 can be implemented even if the names of E-ISAC and NCCIC change or a different agency takes over their current roles.

Requirement R4

General Considerations for Requirement R4

Requirement R4 is a new requirement focused on mandatory reporting of Reportable Cyber Security Incidents and includes attempts to compromise systems in the "Applicable Systems" column. Previously, CIP-008-5 defined reporting requirements for Reportable Cyber Security Requirements (Requirement R1 Part 1.2) only.

Required Reportable Incident Attributes

Requirement R4.1 specifies that initial notifications and updates must include three attributes: 1) functional impact, 2) attack vector used, and 3) level of intrusion achieved or attempted. These attributes are taken directly from the Order. (FERC Order No. 848, paragraph 89).

The SDT understands that some or all of these attributes may be unknown at time of initial notification. To account for this scenario the SDT included "to the extent known" in the requirement language. There is an expectation that update reporting will be done as new information is determined or unknown attributes become known by the entity. There could be cases, due to operational need, that all the attributes may never be known, if this case presents itself that information should be reported.

Methods for Submitting Notifications

Requirement R4 Part 4.2 allows responsible entities to submit notification using any method supported by E-ISAC and NCCIC. The SDT did not prescribe a particular reporting method or format to allow responsible entities' personnel to focus on incident response itself and not the method or format of reporting. It is important to note the report must contain the three attributes required in Requirement R4 Part 4.1 as they are known, regardless of reporting method or format.

Notification Timing

Requirement R4 Part 4.2 specifies two timelines for initial notification submission; one hour for Reportable Cyber Security Incidents; and end of next calendar day for attempts to compromise systems in the "Applicable Systems" column. Paragraph 3 of FERC Order No 848 directly states that reporting deadlines must be established. Paragraph 89 further states that "timelines that are commensurate with the adverse impact to the BES that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES."

- *Reportable Cyber Security Incidents* – The SDT wrote Requirement R4 Part R4.2 to use a one hour deadline for reporting of these events because incidents in this category include successful compromise of ESP(s), EACMS, or BES Cyber System(s). One hour is referenced directly in FERC Order No 848 paragraph 89 and is also the current reporting requirement in CIP-008-5.

- *Cyber Security Incident that was an attempt to compromise one or more systems identified in the "Applicable Systems" column* - Due to the lower severity of these unsuccessful attempts at compromising ESP(s), EACMS, or BES Cyber System(s), the SDT proposed a longer reporting timeframe. The intent behind the decision to add "By the end of the next calendar day" (11:59 pm local time) was to give responsible entities additional time to gather facts prior to notifications for the less severe attempts to compromise Applicable Systems. It is important to note that compliance timing begins with the entity's determination that attempt to compromise meets the process they defined in Requirement R1 Part 1.2.1.

The SDT understands initial notification may not have all the details when first submitted. It is expected, however, that information that has been determined is reported within the notification deadlines. Additionally, it is important to note the wording in Requirement R4 Part 4.2. The "compliance clock" for the report timing begins when the Responsible Entity executes its process from Requirement R1 Part 1.2.1 and a determination has been made that the type of incident which has occurred qualifies as reportable.

Technical rationale taken from the Guidelines and Technical Basis (GTB) CIP-008-5 Requirement 1 provides additional justification for the SDT to maintain the one hour timeframe for Reportable Cyber Security Incidents.

> *"The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."*

In 2007, the Electricity Information Sharing and Analysis Center (E-ISAC) was known as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Its voluntary procedures required the reporting of a cyber-incident within one hour of an incident. CIP-008-1 required entities to report to the ES-ISAC.

In FERC Order No. 706[2] (July 18, 2008), the Commission concluded that the one-hour reporting limit was reasonable [P 663]. The Commission further stated that it was leaving the details to NERC, but it wanted the reporting timeframe to run from the "**discovery**" of the incident by the entity, and not the actual **"occurrence"** of the incident [P 664].

CIP-008-2 and CIP-008-3 were silent regarding the required timeframe for reporting, but it was specifically addressed in CIP-008-5. In the October 26, 2012, redlined version of CIP-008-5, the proposed language for initial notification originally specified "one hour from **identification**" of an incident. This aligned with the Commission's decision in Order No. 706, for the clock to start with the discovery of an incident. However, the Standard Drafting Team changed "one hour from identification" to "one hour from the **determination** of a Reportable Cyber Security Incident". This language was subsequently approved and incorporated into CIP-008-5.

These changes, from "occurrence" to "discovery" to "determination," provide the additional time needed for the entity to apply its specifically created process(es) for determining whether a Cyber Security Incident rises to the level of required reporting. This determination timeframe may include a preliminary investigation of the incident which will provide useful information to other entities to help defend against similar attacks.

---

[2] 2008, Federal Energy Regulatory Commission, Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706.

Notification Updates

Requirement R4 Part 4.3 requires that Responsible Entities submit updates for the required attributes upon determination of new or changed attribute information, if any. The SDT added this language to provide entities sufficient time to determine attribute information, which may be unknown at the time of initial notification, and which may change as more information is gathered. The intent of Requirement R4 Part 4.3 is to provide a method for Responsible Entities to report new information over time as their investigations progress. NOTE: The SDT does not intend updates specified in Requirement R4. Part 4.3 to expose responsible entities to potential violations if, for example, initial and updated notification on the same attribute have different information. This is expected since knowledge of attributes may change as investigations proceed. Rather, the intent of Requirement R4 Part 4.3 is to have a mechanism to report incident information to E-ISAC and NCCIC (and thereby industry) upon determination of each required attribute.

The intent is that the entity report what is known and document the reason not all attributes could become known and ultimately be reported in conditions where, e.g. a Cyber Asset was restored completely, removing all forensic evidence in order to restore operations, which caused the entity to conclude its investigation without having a complete knowledge of the three required attributes.

The SDT asserts that nothing included in the new reporting Requirement R4, precludes the entity from continuing to provide any voluntary sharing they may already be conducting today.

Technical Rationale for Reliability Standard CIP-008-5

This section contains the Guidelines and Technical basis as a "cut and paste" from CIP-008-5 standard to preserve any historical references.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for Reportable Cyber Security Incidents.

Entities may use an actual response to a Reportable Cyber Security Incident as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise.

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for Reportable Cyber Security Incidents. There are several examples of specific types of evidence listed in the measure.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

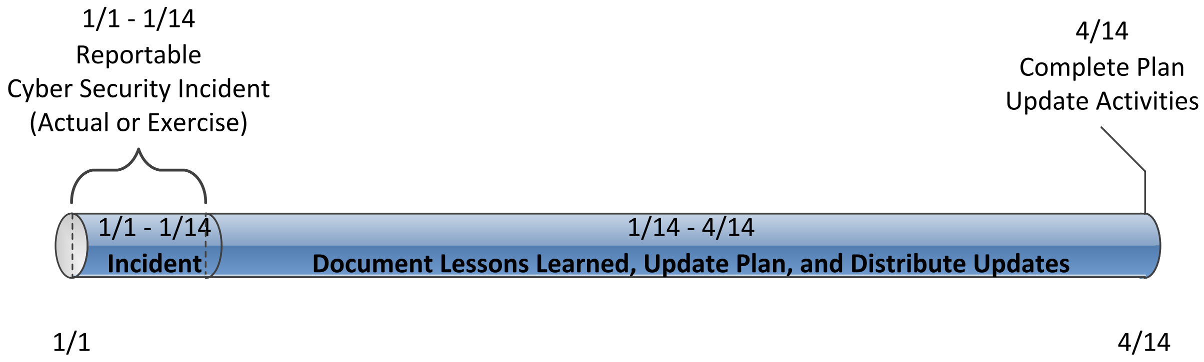
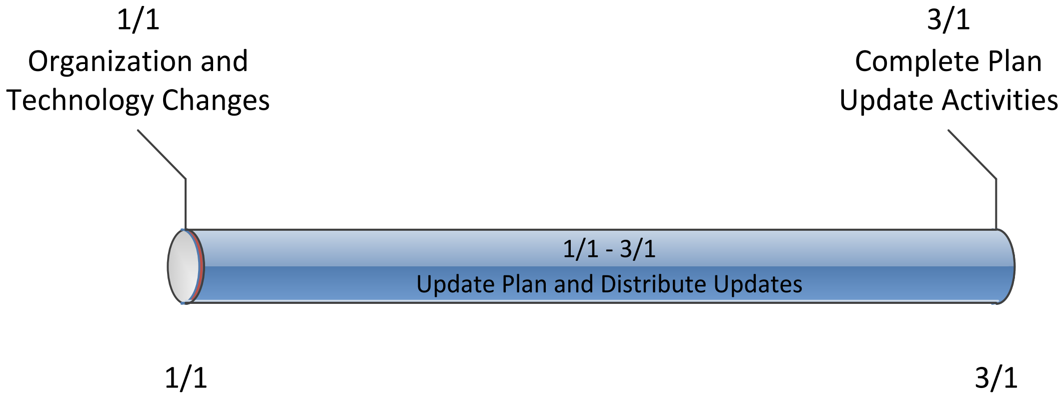


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals.

Figure 2: Timeline for Plan Changes in 3.2



Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)
"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)
Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)
Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)
Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)
Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)
Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)
Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Recovery Plans for BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-009-7

August 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-009-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-009-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-009-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 – Requirement R3

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-009-7 to align recovery planning requirements with the virtualization changes and Shared Cyber Infrastructure (SCI).

The use of the term BES Cyber System has been replaced with "Applicable System" within the requirement language of Requirement R1 Part 1.3 and Requirement R2 Part 2.2 to align the requirement with the applicability for each Requirement Part.

Requirement R1 Part 1.5 has added 'SCI supporting an Applicable System in this Part' to the applicability. This requires that SCI be included in the process to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Having any SCI included in the forensics for a compromised applicable VCA, or the SCI itself, is the reason for the inclusion.

SCI is not specifically included in any other Requirement Parts of CIP-009, because CIP-009 focuses on the ability to recover the BCS functionality, which may or may not require recovery of SCI. The SDT has therefore not included SCI as a direct object of the other recovery plan Requirements and Parts. However, if recovery of the Applicable System's functionality is dependent on recovery of any SCI, then the recovery plan(s) should include such dependencies.

Former Background Section from Reliability Standard CIP-009-6

The section has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.

An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-009-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-009-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Tabletop exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

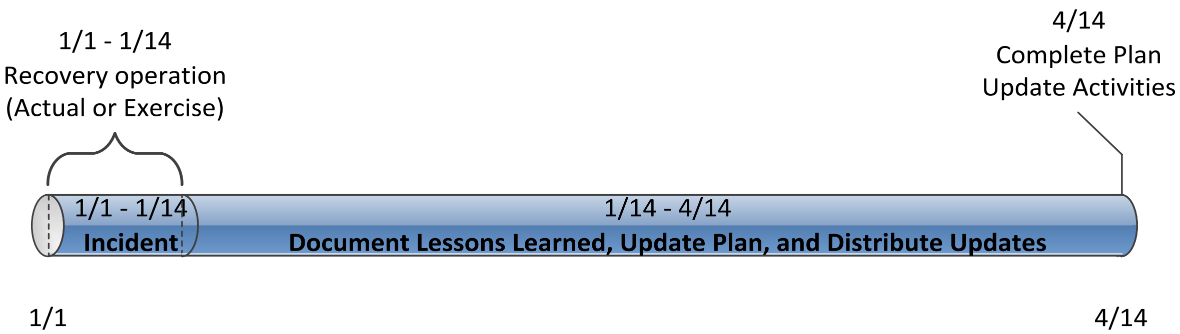


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

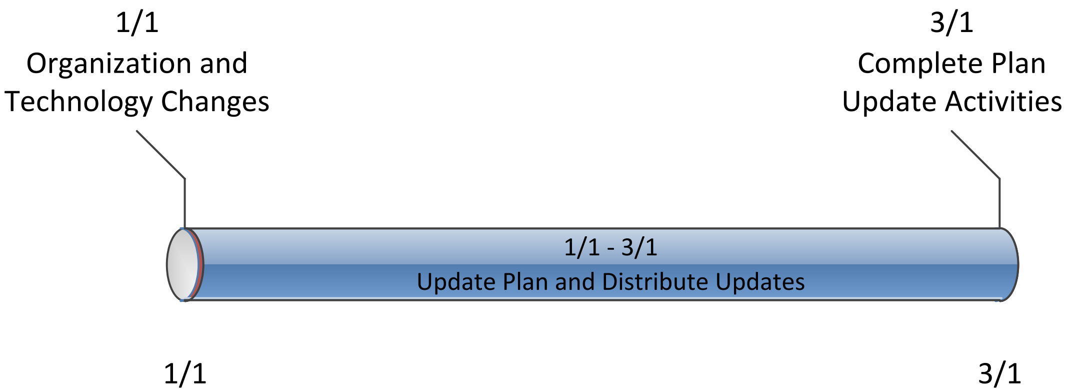


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-5

August 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-010-5

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-5. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-010-5 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

The proposed changes in CIP-010-5 from the Project 2016-02 SDT concern the use of several facets of virtualization technologies. Virtualization allows for such technologies as new controls for Shared Cyber Infrastructure (SCI), remediation VLAN, parent/child images, and dormant virtual machines (VMs). Enabling and clarifying the use of these technologies is the basis of the proposed changes in CIP-010-5. A general introduction to each of these technologies follows.

Shared Cyber Infrastructure (SCI)

Where entries elect to utilize "Shared Cyber Infrastructure" (vs. all in), virtualization abstracts the software layers (the OS and applications Shared Cyber Infrastructure) from the underlying hardware to allow for hardware to be shared among several Virtual Cyber Assets (VCAs) that may be of differing impact levels. Hypervisors include security controls to keep these workloads logically isolated from one another and their requirements are within other CIP standards such as CIP-005 and CIP-007. However, with any type of shared infrastructure, the need for change management requirements is elevated for those security controls that allow for the 'shared' in SCI. Such controls are added to the change management requirements in CIP-010-5.

Remediation VLAN

Remediation VLAN is a term used to describe a logical network segment in which a Cyber Asset or VCA can be isolated from having routable connectivity to any BES Cyber Systems while it is examined to ensure the integrity and validity of the configuration and software installed on it. After this examination and subsequent remediation of deficiencies is completed, it is then permitted routable connectivity to BES Cyber Systems.

This examination is policy driven, meaning that the administrator is able to configure what the minimum requirements are for a successful examination. Examples of this might be minimum operating system patch levels or recent anti-virus definitions.

If during the examination of the asset, it is found to not comply with the requirements defined in the policy, an administrator may intervene to manually remediate the deficiencies, or the system which was used to examine the asset may communicate the deficiencies to the asset with instructions on how to remediate itself in an automated fashion. After the remediation actions are taken, the asset can request to be re-examined and if the requirements dictated by the policy are now met, it will be permitted routable connectivity to BES Cyber Systems

Parent/Child Images

When a VCA is ‘powered on’ or begins execution, it instantiates (“boots”) from a disk image file. Since the boot ‘disk’ is a file and not physical disk, many individual VCAs can use the same “parent” image as the basis for their own “child” image. Among other things, this allows for patching of an OS to occur to a parent image and the child images then pick up that patched image upon their next instantiation.

Dormant VMs

A VCA that is not currently executing or instantiated (i.e., not ‘booted up’) is a dormant VM. It exists not as a traditional VCA, but simply as a file. VCA’s can be created for specialized purposes such as to run troubleshooting tools and only executed or instantiated when needed with long periods of times in between, during which they exist as a file. They are not up and running and on the network where they are managed and patched on a regular basis. However, these can go hand-in-hand with remediation VLANs which would bring them up to date as soon as they do begin to start execution or instantiate, but before they have routable connectivity to BES Cyber Systems.

General Considerations

SCI is mutually exclusive from Cyber Assets (CA) by definition. To enable CIP-010-5 for virtualization, the SDT evaluated the existing Applicable Systems and added “SCI that supports an Applicable System in this Part”. This approach keeps the SCI applicability parallel to each existing variant of Medium Impact BCS (i.e. Medium Impact BCS vs. Medium Impact BCS with External Routable Connectivity (ERC) vs. Medium Impact BCS at Control Centers etc.).

Requirement R1

General Considerations for Requirement R1

In prior versions, CIP-010 Requirement R1 has required developing a baseline configuration that consisted of five (5) items (OS, installed and custom software, ports, patches). The baseline configuration was then used in the remainder of Requirement R1 and R2 as the basis of change management including testing. At a high level, the CIP-010-4 Requirement Part 1.1 was to develop a baseline configuration, Requirement R1 Part 1.2 was to authorize and document changes to the items in the baseline configuration, and Requirement R1 Part 1.3 was to update the baseline configuration within a specific timeframe after a change. This tended to focus the requirement on documenting past changes.

In CIP-010-5, as the SDT considered the more policy-based and automated virtualization technologies discussed in the previous section, the SDT determined to change the focus of Requirement R1 towards a security objective of controlling the implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007, rather than mandating the maintenance of a baseline configuration. Maintaining baseline configurations remains one possible "how", but it is no longer the only prescribed method. The phrase "baseline configuration" has been removed from CIP-010-5 as a result. The items found in the CIP-010-4 baseline are now included in the Measures column within CIP-010-5.

In order to maintain backwards compatibility with CIP-010-4, an entity should document the reasoning of how maintaining of their existing "baseline configuration" meets the stated security objective of controlling the implementation of intended changes to software or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007. Entities may wish to reference NIST SP 800-128 "Guide for Security-Focused Configuration Management of Information Systems" as a guide for additional information.

This change allows the ability to have some backwards compatibility with CIP-010-4 while allowing flexibility for virtualization technologies that automate changes and provide new items (i.e., remediation policies, parent images, etc.) that require change management that were not enumerated in CIP-010-4. This also ensures the focus is not on documenting past changes but the authorization of intended changes, thus making the requirement forward looking with a clearer security objective.

Rationale for Requirement R1 Part 1.1

Conforming changes to Applicable Systems (see General Considerations above).

The original CIP-010 Requirement R1 Part 1.1 included establishing a baseline configuration for assets that included a set of items that would then be monitored for changes in the remaining parts of Requirement R1. Requirement R1 Part 1.1 is similar to what used to be Requirement 1 Part 1.1 - 1.4, and now serves as the focus of the R1 controls.

Requirement R1 Part 1.1 is focused on controlling the implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007. The authorization of those changes (Part 1.1.1) and verifying that the controls are not adversely impacted (Part 1.1.2).

Note that the scope of intended changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.

While a Responsible Entity can benefit from documenting the configuration or the various elements of the previous "baseline", this is no longer a requirement on its own. Maintaining this documentation is now one possible control to use to ensure changes to those elements are managed as required.

Dormant VMs were a challenge with the CIP-010-4 focus on baseline documentation, since the dormant VM is really just a file on disk, and as such cannot impact the BCS until it begins execution or is instantiated, at which time it must be compliant with the requirement. In many cases dormant VMs are patched to current prior to being allowed routable connectivity to BES Cyber Systems. By focusing the Part 1.1 requirement on change management as opposed to documentation of a current configuration, the challenge is mitigated. The Registered Entity must still know what is current, in order to know what security controls are impacted, but the obligation to keep documentation up to date for a dormant VM is removed.

Rationale for Requirement R1 Part 1.2

Requirement R1 Part 1.2 is where CIP-010-4 Requirement R1 Part 1.5 now lands in CIP-010-5, with minor modifications to Part 1.2.1, and conforming changes to remove the 'baseline configuration' terminology to enable for virtualization.

The SDT chose to remove the reliance on a “Technical Feasibility Exception” in favor of permitting “CIP Exceptional Circumstances” in Pat 1.2.1. The SDT contends testing in a test environment prior to implementing any change in production, and documenting test results may impede Responsible Entities' efforts to recover from events or conditions that qualify as CIP Exceptional Circumstances, and that term still requires an entity to document when that condition occurs with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception (TFE).

Additionally, the SDT chose to add to the phrase “that minimizes differences with the production environment” to eliminate the dependency on baseline configuration.

Rationale for Requirement R1 Part 1.3

Conforming changes to Applicable Systems (see General Considerations above).

Requirement R1 Part 1.3 is where CIP-010-4 Requirement R1 Part 1.6 now lands in CIP-010-5, with conforming changes to remove the ‘baseline configuration’ terminology and instead referring to operating systems, firmware, software, or software patches changes as the trigger for the Requirement Part.

The SDT acknowledges virtualization vendors may provide a “golden image” to clone multiple other Virtual Cyber Assets as described in the “Parent/Child Images” section above. The SDT intent is for entities that use the golden image technology to account for the software source and integrity of the golden image which covers any unmodified clones derived from it.

Requirement R2

General Considerations for Requirement R2

Conforming changes to Applicable Systems (see General Considerations above).

The SDT has added the term “unauthorized” into Requirement R2 Part 2.1 to focus it on the risk of unauthorized changes. Many implementations will perform this task by monitoring all changes and looking for unauthorized changes within that population. However, if a way to filter out authorized changes can be implemented, and an entity is able then to have methods to monitor just unauthorized changes the SDT’s intent is that should fulfill the requirement. The scope of this requirement is tied back to Requirement 1 Part 1.1 and is limited to unauthorized changes to software, or unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007.

The SDT also added “per system capability” in recognition that not all changes in scope can be monitored

Requirement R3

Rationale for Requirement R3 Part 3.1

Conforming changes only to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.2

Conforming changes to Applicable Systems (see General Considerations above).

The SDT chose to remove the reliance on a “Technical Feasibility Exception” in favor of the updated term “per system capability”. The SDT contends that the term still requires an entity to document the limit to the system’s capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

In Requirement R3 Part 3.2.1, conforming changes have been made to remove the baseline configuration dependency. Additionally, the SDT chose to add to the phrase "that minimizes differences with the production environment" to eliminate the dependency on baseline configuration.

Rationale for Requirement R3 Part 3.3

The timing of when to enforce this Requirement Part has been an interesting chicken and egg problem. With the inclusion of the language "Prior to becoming a new Applicable System…" the SDT contends that it has resolved this issue, and established that before the new system has applicability, i.e. it has an impact to the BES, this requirement part must be fulfilled.

The SDT's intent is to mirror the changes to the Protected Cyber Asset (PCA) definition, and the proposed change mentioned above to the requirement part language to enable the use of remediation VLANs. The concept of "before connecting to a production environment…" is no longer part if this requirement language.

Conforming changes have been made to remove the baseline configuration dependency. The exceptions are "Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System; or CIP Exceptional Circumstances".

Conforming changes made to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.4

Conforming changes made only to Applicable Systems (see General Considerations above).

Requirement R4

General Considerations for Requirement R4

The SDT updated Requirement R4 to include associated SCI into the scope of the required plans for Transient Cyber Assets (TCA) and Removable Media. The SDT also updated Attachment 1, such that the scope is clarified once within Requirement R4, and applies throughout Attachment 1.

Former Background Section from Reliability Standard CIP-010-4

The section has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-010-4

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

---

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

---

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.
With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity’s responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity’s security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity’s plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rationale for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to “model” the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.

- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.

- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Information Protection

Technical Rationale and Justification for Reliability Standard CIP-011-4

August 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-011-4

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-011-4 . It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-011-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

General Considerations

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-011-4 to align information protection requirements with the virtualization changes.

Requirement R1 and R2

Rationale

To enable CIP-011-4 for virtualization, the SDT added “Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part” within the Applicable Systems column of each of the Parts for Requirement R1 – Requirement R2.

Requirement R2 Part 2.1

Requirement R2 Part 2.1 is an objective level requirement focused on protecting BES Cyber System Information (BCSI) rather than ‘Cyber Assets’ and ‘storage media’, and modified to include Requirement R2 Part 2.2. This consolidation creates necessary flexibility, allowing for cryptographic erasure in scenarios where BCSI cannot be mapped to particular disks within virtualized storage, and where BCSI is stored on SCI employing deduplication. This adjustment is also future-looking to better position CIP-011 for the enablement of cloud type scenarios where the disks are owned and/or managed by a third-party as a service to the entity for its BCSI storage, analysis, or use.

Requirement R2 Part 2.2

Requirement R2 Part 2.2 has been deleted because it was consolidated into Requirement R2 Part 2.1.

Former Background Section from Reliability Standard CIP-011-3

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables: Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-011-3

Requirement R1

General Considerations for Requirement R1
None

Rationale for Modifications to Requirement R1:
Requirement R1 still specifies the need to implement one or more documented information protection program(s). The SDT does not intend that this requirement cover publicly available information, such as vendor manuals or information that is deemed to be publicly releasable. Information protection pertains to both digital and hardcopy information.

The SDT clarified the intent of protecting BCSI as opposed to protecting the BES Cyber System(s) and associated applicable systems which may contain BCSI. This was achieved by modifying the parent CIP-011-X R1 requirement language to include “for BES Cyber System Information (BCSI) pertaining to Applicable Systems”.

Rationale for Modifications to Requirement R1, Part 1.1
Requirement R1, Part 1.1, is an objective level requirement focused on identifying BES Cyber System Information (BCSI). The intent of the SDT was to simplify the requirement language from CIP-011-2 Part 1.1.

Rationale for Modifications to Requirement R1, Part 1.2
Requirement R1, Part 1.2, is an objective level requirement focused on protecting and securely handling BES Cyber System Information (BCSI) in order to mitigate risks of compromising confidentiality. The reference to different states of information such as “transit” or “storage” or “use” was removed. The intent is to reduce confusion of Responsible Entities attempting to interpret controls specific to different states of information, limiting controls to said states, overlapping controls between states, and reduce confusion from an enforcement perspective. By removing this language, methods to protect BCSI becomes explicitly comprehensive.

Requirement language revisions reflect consistency with other CIP requirements.

Requirement R2

General Considerations for Requirement R2
None

Rationale for Requirement R2:
The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BCSI upon reuse or disposal.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement 2 has remained unchanged. The requirements are focused more on the reuse and disposal of BCS rather than BCSI. While acknowledging that such BCS and other applicable systems may have BCSI residing on them, the original intent of the requirement is broader than addressing BCSI. This is a lifecycle issue concerning the applicable systems. CIP-002 focuses on the beginning of the BCS lifecycle but not an end. The potential end of the applicable systems lifecycle is absent from CIP-011 to reduce confusion with reuse and disposal of BCSI. The 2019 BCSI Access Management project did not include modification of CIP-002 in the scope of the SAR. This concern has been communicated for future evaluation.

Technical Rational for Reliability Standard CIP-011-2

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-011-2 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section.

However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.
>
> Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.
>
> In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT
Cyber Security — Supply Chain Risk Management
Technical Rationale and Justification for Reliability Standard CIP-013-3

August 2022

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-013-3

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-3. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-013-3 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-013-3 to align supply chain risk management requirements with the virtualization changes.

To enable CIP-013-3 for virtualization, the SDT added "and Shared Cyber Infrastructure (SCI)" to the parent Requirement R1. Additionally, the SDT simplified the applicability in Requirement R1 Parts 1.1 and 1.2 by replacing the long list of applicable systems with a reference to the list in the parent Requirement R1 through the use of this language, "applicable systems listed in Requirement R1". Note: Because CIP-013-3 does not contain the "Table" construct with an "Applicable Systems" column, this term is not defined within Section 4 Applicability; Therefore, where used, "applicable systems" is intentionally not capitalized within the requirement language of Requirement R1 Parts 1.1 and 1.2.

Technical Rationale for Reliability Standard CIP-013-2

This section contains a “cut and paste” of the Technical Rationale for CIP-013-2 standard to preserve any historical references.

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team’s (SDT’s) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission’s Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

---

[1] NERC, “Cyber Security Supply Chain Risks, Staff Report and Recommended Actions”, May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

---

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however, chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

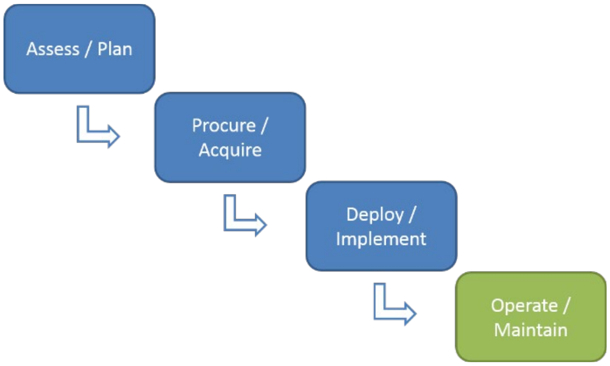
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R3

General Considerations for Requirement R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

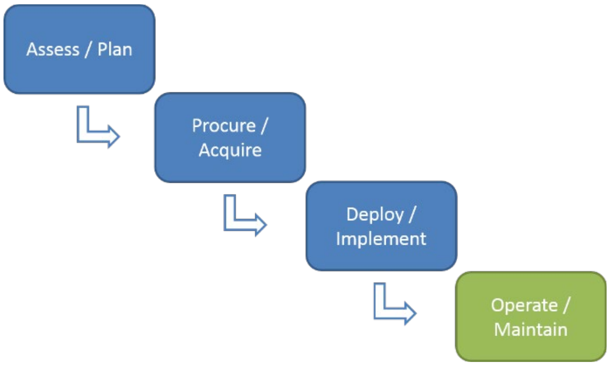
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reminder
Standards Announcement
Project 2016-02 Modifications to CIP Standards | Virtualization

Additional Ballots and Non-binding Polls Open through October 7, 2022

Now Available

The additional ballots and associated Violation Risk Factors and Violation Severity Level non-binding polls for the **CIP Virtualization suite of standards (outlined below)** are open through **8 p.m. Eastern, Friday, October 7, 2022**.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-Y - Cyber Security – Security Management Controls
- CIP-004-8 - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-Y - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Balloting
Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

Note: Votes cast in the previous ballots, will not carry over to additional ballots. It is the responsibility of the registered voter in the ballot pool to vote again. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

UPDATED

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Formal Comment Period Now Open through October 7, 2022

Now Available

The formal comment period for draft 4 of the **CIP Virtualization suite of standards (outlined below)** has been extended and is now open through **8 p.m. Eastern, Friday, October 7, 2022**.

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-Y - Cyber Security – Security Management Controls
- CIP-004-8 - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-Y - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **September 28 – October 7, 2022**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

UPDATED
Standards Announcement
Project 2016-02 Modifications to CIP Standards | Virtualization

Formal Comment Period Now Open through October 7, 2022

Now Available

The formal comment period for draft 4 of the **CIP Virtualization suite of standards (outlined below)** has been extended and is now open through **8 p.m. Eastern, Friday, October 7, 2022**.

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-Y - Cyber Security – Security Management Controls
- CIP-004-8 - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-Y - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **September 28 – October 7, 2022**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Jordan Mallory (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify "Project 2016-02 Modifications to CIP Standards Observer List" in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/258)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 AB 4 ST
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 236
Total Ballot Pool: 303
Quorum: 77.89
Quorum Established Date: 10/7/2022 5:19:27 PM
Weighted Segment Value: 94.63

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	53	0.93	4	0.07	0	5	24
Segment: 2	8	0.6	5	0.5	1	0.1	0	1	1
Segment: 3	66	1	51	0.962	2	0.038	0	2	11
Segment: 4	15	1	10	1	0	0	0	0	5
Segment: 5	74	1	51	0.944	3	0.056	0	3	17
Segment: 6	45	1	32	0.941	2	0.059	0	2	9
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	4	0.4	0	0	0	3	0
Totals:	303	6	206	5.678	12	0.322	0	18	67

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh		None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Negative	Comments Submitted
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 303 of 303 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/258)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 4 ST
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 236
Total Ballot Pool: 303
Quorum: 77.89
Quorum Established Date: 10/7/2022 5:19:36 PM
Weighted Segment Value: 84.9

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	51	0.879	7	0.121	0	4	24
Segment: 2	8	0.6	2	0.2	4	0.4	0	1	1
Segment: 3	66	1	48	0.906	5	0.094	0	2	11
Segment: 4	15	1	10	1	0	0	0	0	5
Segment: 5	74	1	46	0.868	7	0.132	0	4	17
Segment: 6	45	1	32	0.941	2	0.059	0	2	9
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	303	6	192	5.094	26	0.906	0	18	67

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson		None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Third-Party Comments
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc	Todd Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl		None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh		None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson	Amie Shuger McConnaha	None	N/A
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees		None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Affirmative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 303 of 303 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/258)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 4 ST
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 235
Total Ballot Pool: 301
Quorum: 78.07
Quorum Established Date: 10/7/2022 5:15:48 PM
Weighted Segment Value: 84.6

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	53	0.914	5	0.086	0	4	24
Segment: 2	8	0.6	2	0.2	4	0.4	0	1	1
Segment: 3	66	1	47	0.904	5	0.096	0	3	11
Segment: 4	14	1	10	1	0	0	0	0	4
Segment: 5	74	1	45	0.849	8	0.151	0	4	17
Segment: 6	44	1	30	0.909	3	0.091	0	2	9
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	301	6	190	5.076	26	0.924	0	19	66

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Third-Party Comments
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc	Todd Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/258)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 4 ST
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 236
Total Ballot Pool: 301
Quorum: 78.41
Quorum Established Date: 10/7/2022 5:07:31 PM
Weighted Segment Value: 65.26

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	45	0.776	13	0.224	0	4	24
Segment: 2	8	0.6	0	0	6	0.6	0	1	1
Segment: 3	66	1	41	0.788	11	0.212	0	3	11
Segment: 4	14	1	7	0.7	3	0.3	0	0	4
Segment: 5	74	1	38	0.717	15	0.283	0	4	17
Segment: 6	44	1	26	0.765	8	0.235	0	2	8
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	3	0.3	3	0.3	0	1	0
Totals:	301	6.2	160	4.046	59	2.154	0	17	65

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Negative	Third-Party Comments
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Gabe Kurtz		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Third-Party Comments
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Third-Party Comments
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Negative	Comments Submitted
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Boeshaar		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/258)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 AB 4 ST
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 235
Total Ballot Pool: 301
Quorum: 78.07
Quorum Established Date: 10/7/2022 5:15:55 PM
Weighted Segment Value: 92.6

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	55	0.948	3	0.052	0	4	24
Segment: 2	8	0.6	4	0.4	2	0.2	0	1	1
Segment: 3	66	1	49	0.942	3	0.058	0	3	11
Segment: 4	14	1	10	1	0	0	0	0	4
Segment: 5	74	1	50	0.926	4	0.074	0	3	17
Segment: 6	44	1	31	0.939	2	0.061	0	2	9
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	4	0.4	0	0	0	3	0
Totals:	301	6	203	5.556	14	0.444	0	18	66

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Third-Party Comments
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Showing 1 to 301 of 301 entries

Previous 1 Next

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/258)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 4 ST
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 234
Total Ballot Pool: 301
Quorum: 77.74
Quorum Established Date: 10/7/2022 5:20:43 PM
Weighted Segment Value: 67.38

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	45	0.789	12	0.211	0	5	24
Segment: 2	8	0.6	0	0	6	0.6	0	1	1
Segment: 3	66	1	39	0.765	12	0.235	0	4	11
Segment: 4	14	1	8	0.8	2	0.2	0	0	4
Segment: 5	74	1	36	0.706	15	0.294	0	5	18
Segment: 6	44	1	24	0.75	8	0.25	0	3	9
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	3	0.3	2	0.2	0	2	0
Totals:	301	6.1	155	4.11	57	1.99	0	22	67

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Third-Party Comments
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Third-Party Comments
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Third-Party Comments
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Negative	Comments Submitted
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Abstain	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Abstain	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/258)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 AB 4 ST
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 234
Total Ballot Pool: 301
Quorum: 77.74
Quorum Established Date: 10/7/2022 5:20:54 PM
Weighted Segment Value: 95.67

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	56	0.966	2	0.034	0	4	24
Segment: 2	8	0.6	5	0.5	1	0.1	0	1	1
Segment: 3	66	1	50	0.962	2	0.038	0	3	11
Segment: 4	14	1	10	1	0	0	0	0	4
Segment: 5	74	1	50	0.943	3	0.057	0	3	18
Segment: 6	44	1	32	0.97	1	0.03	0	2	9
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	4	0.4	0	0	0	3	0
Totals:	301	6	207	5.74	9	0.26	0	18	67

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/258)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 AB 4 ST
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 234
Total Ballot Pool: 301
Quorum: 77.74
Quorum Established Date: 10/7/2022 5:21:04 PM
Weighted Segment Value: 95.38

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	55	0.948	3	0.052	0	4	24
Segment: 2	8	0.6	5	0.5	1	0.1	0	1	1
Segment: 3	66	1	50	0.962	2	0.038	0	3	11
Segment: 4	14	1	10	1	0	0	0	0	4
Segment: 5	74	1	50	0.943	3	0.057	0	3	18
Segment: 6	44	1	32	0.97	1	0.03	0	2	9
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	4	0.4	0	0	0	3	0
Totals:	301	6	206	5.723	10	0.277	0	18	67

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/258)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 4 ST
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 235
Total Ballot Pool: 301
Quorum: 78.07
Quorum Established Date: 10/7/2022 5:18:32 PM
Weighted Segment Value: 46.35

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	31	0.544	26	0.456	0	5	24
Segment: 2	8	0.6	0	0	6	0.6	0	1	1
Segment: 3	66	1	28	0.549	23	0.451	0	4	11
Segment: 4	14	1	5	0.5	5	0.5	0	0	4
Segment: 5	74	1	25	0.481	27	0.519	0	5	17
Segment: 6	44	1	16	0.5	16	0.5	0	3	9
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	3	0.3	3	0.3	0	1	0
Totals:	301	6.2	108	2.874	106	3.326	0	21	66

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	Comments Submitted
1	Ameren - Ameren Services	Tamara Evey		Negative	Comments Submitted
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Negative	Third-Party Comments
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Negative	Comments Submitted
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Negative	Third-Party Comments
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Third-Party Comments
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Third-Party Comments
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras Sr		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Negative	Comments Submitted
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	East Kentucky Power Cooperative	Chris Adams		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Omaha Public Power District	David Heins		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Negative	Comments Submitted
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Benjamin Winslett		Negative	Comments Submitted
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Negative	Comments Submitted
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Negative	Third-Party Comments
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Negative	Comments Submitted
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	David Melanson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Third-Party Comments
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Abstain	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Negative	Comments Submitted
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Justin Kuehne		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Negative	Comments Submitted
6	Duke Energy	John Sturgeon		Negative	Comments Submitted
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Negative	Third-Party Comments
6	Omaha Public Power District	Shonda McCain		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Southern Indiana Gas and Electric Co.	Erin Spence		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Abstain	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Negative	Comments Submitted
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 301 of 301 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/258)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 AB 4 ST
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 234
Total Ballot Pool: 301
Quorum: 77.74
Quorum Established Date: 10/7/2022 5:21:27 PM
Weighted Segment Value: 82.59

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	52	0.897	6	0.103	0	4	24
Segment: 2	8	0.6	1	0.1	5	0.5	0	1	1
Segment: 3	66	1	47	0.904	5	0.096	0	3	11
Segment: 4	14	1	10	1	0	0	0	0	4
Segment: 5	74	1	44	0.846	8	0.154	0	4	18
Segment: 6	44	1	30	0.909	3	0.091	0	2	9
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	301	6	187	4.956	28	1.044	0	19	67

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Third-Party Comments
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Third-Party Comments
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Showing 1 to 301 of 301 entries

Previous 1 Next

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/258)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 AB 4 ST
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 234
Total Ballot Pool: 301
Quorum: 77.74
Quorum Established Date: 10/7/2022 5:21:41 PM
Weighted Segment Value: 82.88

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	53	0.914	5	0.086	0	4	24
Segment: 2	8	0.6	1	0.1	5	0.5	0	1	1
Segment: 3	66	1	47	0.904	5	0.096	0	3	11
Segment: 4	14	1	10	1	0	0	0	0	4
Segment: 5	74	1	44	0.846	8	0.154	0	4	18
Segment: 6	44	1	30	0.909	3	0.091	0	2	9
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	301	6	188	4.973	27	1.027	0	19	67

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Third-Party Comments
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		None	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Gabe Kurtz		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Third-Party Comments
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Third-Party Comments
2	New York Independent System Operator	Gregory Campoli		Negative	Third-Party Comments
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Third-Party Comments
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Third-Party Comments
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Negative	Comments Submitted
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Negative	Third-Party Comments
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Third-Party Comments
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Justin Kuehne		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Third-Party Comments
6	Constellation	Kimberly Turco		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Simon Tanapat-Andre		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Erin Spence		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	New York State Reliability Council	ALAN ADAMSON		Negative	Third-Party Comments
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Showing 1 to 301 of 301 entries

Previous 1 Next

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 | Non-binding Poll AB 4 NB
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/10/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 224
Total Ballot Pool: 277
Quorum: 80.87
Quorum Established Date: 10/10/2022 9:48:11 AM
Weighted Segment Value: 97.25

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	46	0.958	2	0.042	14	17
Segment: 2	8	0.5	4	0.4	1	0.1	3	0
Segment: 3	63	1	47	0.979	1	0.021	8	7
Segment: 4	14	1	11	1	0	0	0	3
Segment: 5	65	1	41	0.976	1	0.024	8	15
Segment: 6	40	1	25	1	0	0	4	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	3	0.3	0	0	4	0
Totals:	277	5.8	177	5.614	5	0.186	42	53

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Abstain	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Affirmative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Showing 1 to 277 of 277 entries

Previous 1 Next

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 | Non-binding Poll AB 4 NB
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/7/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 210
Total Ballot Pool: 277
Quorum: 75.81
Quorum Established Date: 10/7/2022 7:54:15 PM
Weighted Segment Value: 87.36

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	41	0.911	4	0.089	11	23
Segment: 2	8	0.4	1	0.1	3	0.3	3	1
Segment: 3	63	1	40	0.87	6	0.13	6	11
Segment: 4	14	1	10	1	0	0	0	4
Segment: 5	65	1	36	0.878	5	0.122	7	17
Segment: 6	40	1	22	0.88	3	0.12	4	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	2	0.2	1	0.1	4	0
Totals:	277	5.7	152	4.839	22	0.861	36	67

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		None	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		None	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		None	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		None	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		None	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		None	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 277 of 277 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 | Non-binding Poll AB 4 NB
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/10/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 224
Total Ballot Pool: 277
Quorum: 80.87
Quorum Established Date: 10/10/2022 10:23:54 AM
Weighted Segment Value: 88.46

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	46	0.92	4	0.08	12	17
Segment: 2	8	0.5	2	0.2	3	0.3	3	0
Segment: 3	63	1	41	0.891	5	0.109	10	7
Segment: 4	14	1	11	1	0	0	0	3
Segment: 5	65	1	37	0.881	5	0.119	8	15
Segment: 6	40	1	22	0.88	3	0.12	4	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	2	0.2	1	0.1	4	0
Totals:	277	5.8	161	4.972	21	0.828	42	53

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 277 of 277 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 | Non-binding Poll AB 4 NB
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/10/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 225
Total Ballot Pool: 277
Quorum: 81.23
Quorum Established Date: 10/10/2022 10:23:47 AM
Weighted Segment Value: 69.95

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	34	0.694	15	0.306	13	17
Segment: 2	8	0.5	0	0	5	0.5	3	0
Segment: 3	63	1	32	0.696	14	0.304	10	7
Segment: 4	14	1	9	0.818	2	0.182	0	3
Segment: 5	65	1	31	0.738	11	0.262	8	15
Segment: 6	40	1	20	0.769	6	0.231	4	10
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	277	5.9	128	3.915	55	1.985	42	52

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Negative	Comments Submitted
3	Lakeland Electric	Steven Marshall		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Negative	Comments Submitted
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Chuck Booth		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Jennifer Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 277 of 277 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 | Non-binding Poll AB 4 NB
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/10/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 224
Total Ballot Pool: 278
Quorum: 80.58
Quorum Established Date: 10/10/2022 10:48:13 AM
Weighted Segment Value: 93.44

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	48	0.96	2	0.04	12	18
Segment: 2	8	0.6	3	0.3	3	0.3	2	0
Segment: 3	63	1	44	0.957	2	0.043	10	7
Segment: 4	14	1	11	1	0	0	0	3
Segment: 5	65	1	39	0.929	3	0.071	8	15
Segment: 6	40	1	23	0.92	2	0.08	4	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	3	0.3	0	0	4	0
Totals:	278	5.9	171	5.365	12	0.535	41	54

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc	Chuck Booth		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 | Non-binding Poll AB 4 NB
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/10/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 224
Total Ballot Pool: 278
Quorum: 80.58
Quorum Established Date: 10/10/2022 10:48:17 AM
Weighted Segment Value: 73.08

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	35	0.7	15	0.3	12	18
Segment: 2	8	0.5	0	0	5	0.5	3	0
Segment: 3	63	1	35	0.761	11	0.239	10	7
Segment: 4	14	1	10	0.909	1	0.091	0	3
Segment: 5	65	1	32	0.762	10	0.238	8	15
Segment: 6	40	1	19	0.76	6	0.24	4	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	2	0.2	1	0.1	4	0
Totals:	278	5.8	133	4.092	49	1.708	42	54

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Negative	Comments Submitted
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Negative	Comments Submitted
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Negative	Comments Submitted
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Negative	Comments Submitted
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Showing 1 to 278 of 278 entries

Previous 1 Next

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 | Non-binding Poll AB 4 NB
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/10/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 224
Total Ballot Pool: 278
Quorum: 80.58
Quorum Established Date: 10/10/2022 10:49:00 AM
Weighted Segment Value: 96.7

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	49	0.98	1	0.02	12	18
Segment: 2	8	0.5	4	0.4	1	0.1	3	0
Segment: 3	63	1	45	0.978	1	0.022	10	7
Segment: 4	14	1	11	1	0	0	0	3
Segment: 5	65	1	40	0.952	2	0.048	8	15
Segment: 6	40	1	24	0.96	1	0.04	4	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	3	0.3	0	0	4	0
Totals:	278	5.8	176	5.571	6	0.229	42	54

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc	Chuck Booth		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 | Non-binding Poll AB 4 NB
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/10/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 224
Total Ballot Pool: 278
Quorum: 80.58
Quorum Established Date: 10/10/2022 10:48:51 AM
Weighted Segment Value: 96.15

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	48	0.96	2	0.04	12	18
Segment: 2	8	0.5	4	0.4	1	0.1	3	0
Segment: 3	63	1	45	0.978	1	0.022	10	7
Segment: 4	14	1	11	1	0	0	0	3
Segment: 5	65	1	40	0.952	2	0.048	8	15
Segment: 6	40	1	24	0.96	1	0.04	4	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	3	0.3	0	0	4	0
Totals:	278	5.8	175	5.551	7	0.249	42	54

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc	Chuck Booth		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 | Non-binding Poll AB 4 NB
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/10/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 224
Total Ballot Pool: 278
Quorum: 80.58
Quorum Established Date: 10/10/2022 10:48:47 AM
Weighted Segment Value: 57.46

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	31	0.633	18	0.367	13	18
Segment: 2	8	0.5	0	0	5	0.5	3	0
Segment: 3	63	1	28	0.609	18	0.391	10	7
Segment: 4	14	1	7	0.7	3	0.3	1	3
Segment: 5	65	1	22	0.524	20	0.476	8	15
Segment: 6	40	1	14	0.56	11	0.44	4	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	3	0
Totals:	278	5.9	104	3.225	77	2.675	43	54

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Negative	Comments Submitted
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Negative	Comments Submitted
1	Duke Energy	Laura Lee		Negative	Comments Submitted
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Negative	Comments Submitted
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great River Energy	Michael Brytowski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Hydro One Networks, Inc.	Paul Malozewski		Negative	Comments Submitted
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	David Heins		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Negative	Comments Submitted
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Abstain	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Negative	Comments Submitted
4	LaGen	Wayne Messina	Clay Walker	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Comments Submitted
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Negative	Comments Submitted
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Negative	Comments Submitted
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Selene Willis		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Negative	Comments Submitted
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Comments Submitted
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Jennifer Bennett		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Negative	Comments Submitted
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	John Sturgeon		Negative	Comments Submitted
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Negative	Comments Submitted
6	Omaha Public Power District	Shonda McCain		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 | Non-binding Poll AB 4 NB
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/10/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 225
Total Ballot Pool: 278
Quorum: 80.94
Quorum Established Date: 10/10/2022 10:34:48 AM
Weighted Segment Value: 87.5

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	45	0.9	5	0.1	12	18
Segment: 2	8	0.6	1	0.1	5	0.5	2	0
Segment: 3	63	1	42	0.913	4	0.087	10	7
Segment: 4	14	1	11	1	0	0	0	3
Segment: 5	65	1	38	0.884	5	0.116	8	14
Segment: 6	40	1	22	0.88	3	0.12	4	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	2	0.2	1	0.1	4	0
Totals:	278	5.9	161	4.877	23	1.023	41	53

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Sheraz Majid		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 | Non-binding Poll AB 4 NB
Voting Start Date: 9/28/2022 12:01:00 AM
Voting End Date: 10/10/2022 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 4
Total # Votes: 224
Total Ballot Pool: 278
Quorum: 80.58
Quorum Established Date: 10/10/2022 10:49:18 AM
Weighted Segment Value: 87.98

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	46	0.92	4	0.08	12	18
Segment: 2	8	0.6	1	0.1	5	0.5	2	0
Segment: 3	63	1	42	0.913	4	0.087	10	7
Segment: 4	14	1	11	1	0	0	0	3
Segment: 5	65	1	37	0.881	5	0.119	8	15
Segment: 6	40	1	22	0.88	3	0.12	4	11
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.3	2	0.2	1	0.1	4	0
Totals:	278	5.9	161	4.894	22	1.006	41	54

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Mike Braunstein		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Negative	Comments Submitted
1	CPS Energy	Gladys DeLaO		None	N/A
1	Dairyland Power Cooperative	Steve Ritscher		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Candace Marshall		Affirmative	N/A
1	Duke Energy	Laura Lee		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Julie Severino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		None	N/A
1	Hydro One Networks, Inc.	Sheraz Majid		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	Hydro-Quebec (HQ)	Nicolas Turcotte		None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	James Baldwin		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Abstain	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Abstain	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Kevin Carley		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla		None	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	Gabe Kurtz		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A
1	Western Area Power Administration	Ben Hammer	Barry Jones	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Dana Showalter		Abstain	N/A
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Negative	Comments Submitted
2	New York Independent System Operator	Gregory Campoli		Abstain	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Comments Submitted
3	AEP	Kent Feliks		Abstain	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Michael Dieringer		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ken Lanehome		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Duan Gavel		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Dominion - Dominion Resources, Inc.	Connie Schroeder		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Affirmative	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	Glen Allegranza		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	Abstain	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Adam Menendez		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Abshier		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Benjamin Winslett		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		None	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Scott Winner		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Negative	Comments Submitted
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Rachel Snead		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Adrian Raducea		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Robert Loy		Affirmative	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Carl Pineault		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Jason Fortik		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	NB Power Corporation	David Melanson		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		None	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Abstain	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Meaghan Connell		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Amy Jones		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Jennifer Bennett		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Jim Howell, Jr.		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
6	AEP	Justin Kuehne		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Negative	Comments Submitted
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Donna Stephenson		Affirmative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	New York Power Authority	Anirudh Bhimireddy		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Glen Pruitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Public Utility District No. 2 of Grant County, Washington	M LeRoy Patterson		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Israel Perez		Affirmative	N/A
6	Seattle City Light	Brian Belger		Abstain	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	William Steiner		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 278 of 278 entries

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization - Draft 4
Comment Period Start Date:	8/17/2022
Comment Period End Date:	10/7/2022
Associated Ballots:	2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 AB 4 ST

There were 72 sets of responses, including comments from approximately 188 different people from approximately 121 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

2. The SDT modified other definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

3. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

4. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

5. The SDT has used phrasing such as "SCI supporting an Applicable System from this Part" in the Applicable Systems column across many of the standards. Is it clear that this scopes the requirements for SCI to match the system(s) it hosts?

6. The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

7. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes or scoping clarifications related to SCI. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

8. The SDT has revised the Implementation Plan to include 3 defined early adoption dates as options should Responsible Entities choose to do so. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

9. Please provide any additional comments for the standard drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
WEC Energy Group, Inc.	Christine Kane	3		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC

					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	3,5	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO
					Jamie Monette	Allete - Minnesota Power, Inc.	1	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc.	2	MRO
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					George Brown	Acciona Energy North America	5	MRO

					Jaimin Patel	Saskatchewan Power Corporation	1	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Tricia Bynum	FirstEnergy - FirstEnergy Corporation	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Public Utility District No. 1 of Chelan County	Meaghan Connell	5		PUD No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
California ISO	Monika Montez	2	WECC		Monika Montez	CAISO	2	WECC

				ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Dana Showalter	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	IS-NE	2	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Michael Del Viscio	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SERC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern Company Services, Inc. - Gen	5	SERC
DTE Energy	patricia ireland	4		DTE Energy	Patricia Ireland	DTE Energy - Detroit Edison	4	RF
					Karie Barczak	DTE Energy - Detroit Edison Company	3	RF
					Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
Northeast Power	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional	Gerry Dunbar	Northeast Power	10	NPCC

Coordinating Council				Standards Committee		Coordinating Council		
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Harish Vijay Kumar	IESO	2	NPCC
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC

					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					John Pearson	ISONE	2	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable

					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD / BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC

					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST sees no reason to change the existing definition's use of "remote access client or other remote access technology." The second part of the proposed definition would, as written, apply to any remote connection using a communications path that included routable to serial conversion, regardless of where that conversion took place (e.g., remote location vs. "local," or "inside the BES asset" location). NST is aware of concerns that using phrases such as "outside the asset" in this context might cause confusion about its relationship to electronic access control requirements for BES assets containing low impact BCS, but we nonetheless recommend using it to avoid overly broad application of "IRA" to communications using both routable and serial wide-area connections.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

The term “Cyber System” is too broad in scoping IRA. Suggest revise to clarify that the target of IRA is BES Cyber System rather than “Cyber System” to avoid including EACMS, SCI, PCA, etc.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC

Answer	No
Document Name	

Comment

Under the new definition of IRA, bullet 5 that excludes “Communication that originates from an Intermediate System; or,” should not be excluded from the definition. Excluding it would be confusing as IRA to a BCS should come from an Intermediate System.

The new definition of IRA conflicts with the existing definition of ERC. ERC is the ability to access a BCS through its ESP via a “bi-directional” routable protocol connection.

In the new IRA definition, the second bullet addressing serial Cyber Assets states that IRA is “User-initiated electronic access by a person using a routable protocol” (*not necessarily bi-directional*), “that is converted by the Responsible Entity to a non-routable protocol….,” is in direct conflict with the existing definition of ERC. This is not a concern over serial end points being in scope or not, we all agree that they are in scope, but the term “bi-directional” does nothing to help bring serial devices into scope, in fact it implies that serial devices that do not establish TCP/IP connections are out of scope.

Our recommendation to the SDT is to modify the definition of ERC as follows. First, remove the words “bi-directional” since there is no such thing as bi-directional routable protocol. Changing the ERC definition to simply “routable protocol” would create consistency throughout the requirements. Second, remove the word “connection” as this term implies that there has been a TCP handshake and a connection is established while excluding connectionless protocols such as UDP. Consider using “routable protocol communication” or just “routable protocol”. In CIP-005 R1.2, reference is made to routable protocol communication instead of connection, so the SDT may want to align with that if they are using the term routable protocol is not enough.

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

Should “or” be added to the end of the first bullet to more clearly define the need to continue dropping through the bullets like a decision tree to identify if any of the points are true instead of exiting after the first question? It is unclear if after the first bullet is an “and” or an “or” to identify IRA.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Changes to the IRA definition adds conversion from routable to non-routable (serial) communications to remote BCS that was previously omitted. Further clarifications in the definition of IRA removes some gray areas and further delineates IRA from system-to-system communications. However, there remains a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication but have not enforced protections to ensure that malicious actors do not use the ports – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to the definition to ensure validity of communications to Applicable Systems regardless of source or intent. In addition, approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization and approval of SCI terminology and other definitions associated with virtualization.

The SDT has added rationale but not defined whether user-created scripts and programs that can be modified and scheduled to run independently are considered IRA – even though an unauthorized user could modify it to their benefit. Both scripts and programs can be user-initiated, and with no definition of system-to-system communications there are still lingering issues regarding what system-to-system communications is comprised. Further, user-created scripts and programs may not be capable of reading multi-factor tokens or their displayed codes, but additional security for these connections can be implemented through certificates and the use of secure connections via SSH or SSL.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

The revised definition of IRA provides more clarity than the earlier version. With that said, AEP recommends removing second bullet under what “IRA does not include” list, as IRA should include “communication that originates from an Intermediate System”.

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

Request confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC

Likes 0

Dislikes 0

Response

Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC

Answer No

Document Name

Comment

Suggest change to ¨To a Management Interface of Shared Cyber Infrastructure protected by an ESP¨. As management interface of target SCI should be located inside ESP and SCI outside ESP should not be in scope.

Request confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC

Likes 0

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer No

Document Name

Comment

Request confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC.

Likes 0

Dislikes 0

Response

Jodirah Green - ACES Power Marketing - 6

Answer No

Document Name

Comment

The IRA definition contains “To a Manangement Interface of Shared Cyber Infrastructure”. We feel this should read “To a Management Interface”. Adding SCI to the definition restricts the scope to just Management Interfaces on SCI. Management Interface’s definition contains SCI, so it is unnecessary to put SCI into the requirement as well.

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

We suggest that IRA definition should remain unchanged and have the specific scenarios that these definition changes are attempting to address become part of the standard requirement language. (i.e. CIP-005-8 R2).

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

Request confirmation that entities should re-evaluate serial connections because they may now be in scope due to the updated definitions of IRA and ERC.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)

Answer	No
Document Name	

Comment

The SRC suggests that IRA definition should remain unchanged and have the specific scenarios that these definition changes are attempting to address become part of the standard requirement language. (i.e. CIP-005-8 R2).

1. The SDT modified other definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern agrees with the proposed changes for the IRA definition.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the IRA definition modifications.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	Yes
Document Name	

Comment

WECC suggests that the CIP-005-8 R2.4 use of ‘vendor remote access’ in the applicable system is not consistent with ‘active vendor remote access sessions’ and causes confusion considering neither term is defined. WECC suggests removing ‘vendor remote access’ from the applicable systems and have the scope of ‘active vendor remote access sessions’ stand on its own.

Likes 0	
Dislikes 0	

Response

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

SIGE agrees with the revisions to the IRA definition. Use of an Intermediate System to access systems that convert routeable to non-routable protocol adds a mandatory MFA step that may not be present in current implementations, and logs use of those systems.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) agrees with the revisions to the IRA definition. Use of an Intermediate System to access systems that convert routeable to non-routable protocol adds a mandatory MFA step that may not be present in current implementations, and logs use of those systems.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment	
Xcel Energy supports EEI comments and thanks the SDT for the hard work in developing this definition.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the revised Interactive Remote Access (IRA) definition.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Chelan appreciates the SDT's work on IRA and CIP-005 and approves the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	

Kimberly Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	Yes
Document Name	

Comment

Kimberly Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	Yes
Document Name	

Comment

Thank you to the SDT for clarifying what is and what is not applicable.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the revised definition of IRA.

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	Yes
Document Name	

Comment

MRO does not understand the need for the qualifier ‘by the Responsible Entity’ added to the conversion to non-routable. This seems like it would give entities a way out of compliance with the IRA requirements around serial communication by having someone else convert it.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

Cleco agrees with EEI comments.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - Pedernales Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer

Document Name

Comment

Suggest change to ¨To a Management Interface of Shared Cyber Infrastructure protected by an ESP¨. As management interface of target SCI should be located inside ESP and SCI outside ESP should not be in scope.

Request confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC

Likes 0

Dislikes 0

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer

Document Name

Comment

“See comments submitted by the Edison Electric Institute”

Likes 0

Dislikes 0

Response

2. The SDT modified other definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No: Application Containers need to be defined with additional clarity.	
Likes 0	
Dislikes 0	
Response	

Bradley Collard - Pedernales Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
PEC would like to see the SDT provide clarity regarding virtual machines on a TCA being treated as software, however a VCA running on an SCI is not software, but a CA.	
Likes 0	
Dislikes 0	
Response	

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
The phrase “actively remediated in an environement” in the PCA and VCA definitions needs to be clarified; additional information on the meaning of that phrase that was included in the technical rationale could be utilized to clarify the definitions. For CIP-003, Attachment 1, Section 4, request confirmation that, while this Section has no updates, this Section’s scope is being expanded because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident.	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	No
Document Name	
Comment	
See comments from question 1.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro appreciates the opportunity to review and offers the following comments. PCA definition needs clarification. The second bullet refers to a cyber asset being remediated in an isolated environment. It is unclear what remediation and isolation is required. An use case and example would be helpful to explain the intent here.	

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren believes that in the BCSI definition, Shared Cyber Infrastructure should be put in parentheses so that it's clear that SCI is a part of BCSI.	
Likes 0	
Dislikes 0	
Response	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	No
Document Name	
Comment	
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section’s scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section’s scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident	
Likes 0	

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer No

Document Name

Comment

AEP supports all proposed definitions with the exceptions of “Cyber Assets” and
“Interactive Remote Access (IRA)”. Our comments are specified below:

- **Cyber Assets**: The SDT added “*Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets*” to the definition of Cyber Asset. AEP suggests deleting the added sentence since it adds more confusion to the definition and it is included in the VCA definition.
- **Interactive Remove Access (IRA)**: Please see our response under Question #1.

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer No

Document Name

Comment

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes. Further, introducing Shared Cyber Infrastructure (SCI) and Management Interface increases the number of Requirements and Parts that a Responsible Entity needs to track compared to simply identifying the hypervisor and associated hardware and “high-water marking” them with the highest identified impact rating BCA/VCA, EACMS, or PACS, and creating a BCS.

Further, the ideology surrounding “remediation VLANS” should be revisited to understand the risks posed by implementing such an environment. The complexity required to balance these pooled resources using affinity rules or logical boundaries to disallow different impact levels of VM guests from running on the same physical resources could be high. RF believes that the rationale put forth by the Standards Drafting Team for a “remediation VLAN” and the use of automation of security controls poses additional risks that can be mitigated through the use of Transient Cyber Assets (TCAs) in CIP-010 to accomplish the same vulnerability assessments and updates (OS patches, AV updates, etc.) without the complexity or risk associated with having to identify and unidentify PCAs as they are taken out and placed into service in the production network.

Likes 0

Dislikes 0

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

The current definition of “Management Interface” still appears to be a bit unclear. It seems to exclude the management interface of a switch inside the Electronic Security Perimeter. NRG recommend changing the third bullet of the definition from “Configures an Electronic Security Perimeter” to “Configures a network device.”

Additionally, the proposed “Protected Cyber Assets” definition could be read to include any Virtual Cyber Asset that shares physical CPU or memory, despite the addition of “resources”. We believe the intent of the drafting team to be sharing virtual CPU or memory. If so, the definition should be clarified to read, “any Virtual Cyber Asset sharing the same CPU or memory allocation.”

Likes 0

Dislikes 0

Response

Kristine Martz - Amazon Web Services - 7

Answer	No
Document Name	

Comment

AWS agrees with the following proposed definition changes but asks the SDT to consider including the items suggested below in implementation guidance to support entities in adopting the revised definitions:

Interactive Remote Access (IRA): AWS asks the SDT to consider including the meaning of system-to-system communications in implementation guidance to support entities with implementing the revised IRA definition. We suggest including elements such as where the system-to-system communication originates – inside or outside of the Electronic Security Perimeter (ESP).

Management Interface: AWS asks the drafting team to consider clarifying the meaning of “administrative interface.” For example, the SDT could clarify if “administrative interface” is intended to include Graphical User Interfaces (GUIs), Command Line Interfaces (CLIs), Software Development Kits (SDKs), and/or Application Programming Interfaces (APIs).

Virtual Cyber Asset (VCA): AWS asks the SDT to consider including the meaning of “dormant file-based images” in implementation guidance to support entities with implementing the revised VCA definition. Additionally, AWS suggests including guidance to ensure that security controls are in place for dormant file-based images to mitigate vulnerabilities. For example, guidance that includes verification that required cyber security controls are in place prior to using the file-based image in production.

AWS does not agree with the following proposed definition:

Transient Cyber Asset (TCA): The modification to the Transient Cyber Asset definition that allows virtual machines running on a physical TCA to be treated as software on the device should be reconsidered. As written, an entity may not apply the appropriate security controls to the virtual machines running on physical TCAs. Entities should be monitoring the state of the virtual machines running on their physical hardware for security issues. We propose removing the language “Virtual machines hosted on a physical TCA can be treated as software on that physical TCA” from the TCA definition. By removing this language, entities would be required to apply security controls to the virtual machines hosted on their physical TCAs in alignment with CIP-010 R4.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

The current definition of “Management Interface” still appears to be a bit unclear. It seems to exclude the management interface of a switch inside the Electronic Security Perimeter. NRG recommend changing the third bullet of the definition from “Configures an Electronic Security Perimeter” to “Configures a network device.”

Additionally, the proposed “Protected Cyber Assets” definition could be read to include any Virtual Cyber Asset that shares physical CPU or memory, despite the addition of “resources”. We believe the intent of the drafting team to be sharing virtual CPU or memory. If so, the definition should be clarified to read, “any Virtual Cyber Asset sharing the same CPU or memory allocation.”

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	No
Document Name	

Comment

The definition of Protected Cyber Asset carries with it an implicit requirement with the CPU and memory clause. The implication of the requirement is that a VM that is not a Protected BES Cyber Asset may not share CPU and memory with a BES Cyber System. If out-of-scope VM inadvertently shares CPU and memory with a BES Cyber System, then it suddenly becomes a PCA by definition and has instantly violated the majority of the CIP requirements. This is similar to the issue with Intermediate System that was corrected in this draft.

Chelan recommends removing the CPU and memory sharing clause and adopt the suggested language in Q4 for CIP-007 R1.3, a requirement that a BCS/PCA may not share CPU and memory with non-BCS/PCA of the same impact level. That would change an inadvertent resource sharing incident into a single violation of CIP-007 R1.3 rather than violating all the requirements that have PCA as an Applicable System. Please see the response to question 4 for suggested language.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	No
Document Name	

Comment

WEC Energy Group has a continued concern with the newly defined term "Management Interface". Based on the rationale, it is understood why the need to define these interfaces exists. However, this definition differs from the virtual concept and extends to application functionality tools which, in our opinion, is outside of the intended scope of the Project. Thus bringing additional devices into scope even for those entities that are not using virtual machines. Proposing the SDT remove the 3rd bullet from the definition.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC

Answer	No
Document Name	

Comment

While updating the definition of EAP for virtualization and to accommodate zero trust architectures, it would be good to also not refer to a “Cyber Asset interface,” as the EAP could be a zone-based implementation, transparent firewall, a single physical interface, multiple physical interfaces, sub interfaces (virtual SVI) or a port channel/group. The term Cyber Asset “interface” is too restrictive.

We recommend the SDT change the definition to “An electronic access or policy enforcement point on an EACMS that controls routable communication to and from one or more BES Cyber Systems and their associated PCAs.”

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	No

Document Name	

Comment

Manitoba Hydro thanks the drafting team for considering all comments and implementing changes to the definitions. Manitoba Hydro is in support of the changes to most definitions and the new definitions. For the updated definition of **Electronic Access Control or Monitoring Systems (EACMS)** it appears that the scope has inadvertently been increased with the “SCI” wording. The definition includes Cyber Assets… that perform electronic access control or electronic access monitoring of… SCI. The definition for SCI includes systems that host EACMS and PACS and systems that provide storage resources to EACMS and PACS. The scope of an EACMS would therefore increase to include systems that provide electronic access control and monitoring for SCI supporting EACMS and PACS, however systems providing electronic access control and monitoring directly for EACMS and PACS are not in scope. The definition is the only place where the scope of EACMS is set.

The following wording is suggested:

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s), BES Cyber Systems or SCI supporting applicable Cyber Assets. This includes Intermediate Systems.

Manitoba Hydro also notes a minor clarification in the new definition of Management Interface. It referest to deploying “SCI”, this should actually refer to the VCA hosted on the SCI:

An administrative interface that:

• Controls the processes of initializing or deploying VCA hosted on SCI or

Controls the process of configuring Shared Cyber Infrastructure; or

• Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or

• Configures an Electronic Security Perimeter.

Additionally the definition for VCA includes the term “virtual machine”. This is a technology specific term and excludes some potential instances of VCA such as virtualization used in the CISCO Nexus platform. This can be resolved by removing the following wording: “currently executing on a virtual machine”

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No

Document Name	

Comment

In the proposed definition of “Cyber Asset”, the definition of “application container” versus VCA is unclear. The term “container” used in this definition needs further clarification.

In the proposed definition of “Management Interface”, the definition of “administrative interface” is unclear. The term “administrative interface” used in this definition needs further clarification.

In the proposed definition of TCA, removal of the qualifier “directly” may inappropriately expand the scope of the requirement to include devices connecting via IRA or Intermediate System.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

Definition of VCA: NST believes the proposed definition of VCA should more closely resemble the existing definition of "Cyber Asset" or, better still, be eliminated altogether. The existing definition of "Cyber Asset" could be easily "unbound" from "hardware" with this or a similar modification:

Change from, "Programmable electronic devices, including the hardware, software, and data in those devices" to, "Hardware-based or virtual programmable electronic devices, including the software and data in those devices."

Definition of TCA: NST considers the statement in the proposed definition of TCA, "Virtual machines hosted on a physical TCA are treated as software on that physical TCA" to be oddly inconsistent with the proposed definition of VCA. Furthermore, we disagree with the SDT's opinion that if a physical TCA hosts one or more virtual TCAs, there should be no need to track and manage each individual physical and virtual device.

Definition of ESP: NST believes the proposed new part of the current ESP definition, “or a logical boundary defined by one or more EAPs” is redundant and unnecessary. We therefore recommend maintaining the currently approved ESP definition.

Definition of ERC: NST believes the use of the word, "through (an ESP)" has the potential to cause confusion over what kind of routable communications qualify as ERC. ERC to or from a Cyber Asset should be clearly defined as "through" an ESP boundary or access point, not "through" an ESP (the online Merriam Webster dictionary defines "through" as "a function word to indicate movement into at one side or point and out at another and especially the opposite side of // 'drove a nail through the board'"). NST believes the existing definition of ERC can and should be retained as-is.

Definition of EAP: NST believes the proposed definition of EAP is problematic in two respects. First, we believe it could be interpreted to mean an EAP should control all routable communication between a BCS and any other Cyber Asset regardless of whether that "other" device is within or outside of

the same ESP protecting the BCS. Second, we believe the SDT should better define "policy enforcement point," lest Responsible Entities, Regional Entities, and NERC develop their own conflicting definitions.	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
Greater clarity is needed regarding Cyber Assets, CIP Systems and Cyber Systems. The differences between these terms should be made more explicit, overlaps should be eliminated, and redundant terms should be eliminated also.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

“Management Interface” – the language of the definition still leaves ambiguity of interfaces on other CAs, for example vCenter. It is understood that the intent of the SDT was to only include interfaces on applicable CAs, which could leave those unprotected by the standards.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the modified definitions used in the CIP standards.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	Yes
Document Name	

Comment

- NextEra Energy (NEE) encourages the SDT to enhance the clarification of bi-directional routable communication with IRA and ERC. Entities will need to clarify their implementation of bi-directional for routable communications.
- Is requiring authentication to a local network or different VLAN considered a logical break?

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	Yes
Document Name	

Comment

Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the modified definitions that will be used for the CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for the hard work in developing these definitions.	

Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE recommends consistent use of “Shared Cyber Infrastructure (SCI)” throughout the definitions.	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
The only disagreement with the proposed defintions is for the CIP Senior Manager. The updated definition for CIP Senior Manager could cause some confusion because it is broad and appears to apply to all the CIP Standards, even though CIP-012 and CIP-014 do not have CIP Senior Manager requirements or responsibilities. An alternate wording could be “…. continuing adherence to the requirements within the NERC Critical Infrastructure Protection Standards in which the CIP Senior Manager has responsibilities"	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE recommends consistent use of “Shared Cyber Infrastructure (SCI)” throughout the definitions.	

Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the modifications to the definitions, however, would like additional clarity on the meaning of “application container” which is used within the definitions.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the proposed changes of the CIP standards definitions. Suggestions for updates have been listed below.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	

Likes 0

Dislikes 0

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE is concerned the proposed definition of Electronic Access Point (EAP) is ambiguous. Texas RE believes the SDT's intent was to write a definition that applied to communications between BES Cyber Systems and PCAs and Cyber Assets not protected by the same ESP. The proposed definition as written, however, could be interpreted to mean that EAPs are only applicable when controlling communication between a BCS and its PCAs. The proposed language as written could also be interpreted to mean "An electronic policy enforcement point" or "a Cyber Asset interface on an EACMS that controls routable communication to and from one or more BES Cyber Systems and their associated PCAs."

It could also be interpreted to mean "An electronic policy enforcement point" or "a Cyber Asset interface on an EACMS that controls routable communication to and from one or more BES Cyber Systems and their associated PCAs.

For clarification, Texas RE recommends the following definition:

An EAP is:

- A Cyber Asset interface on an EACMS; or
- An electronic policy enforcement point

that controls routable communications between Cyber Systems protected by an ESP and:

- one or more Cyber Systems that are not protected by an ESP; or
- one or more Cyber Systems that are protected by a different ESP.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	
Document Name	

Comment

For definition of Transient Cyber Asset (TCA): Reconsider the wording of the sentence ¨ Virtual machines hosted on a physical TCA are treated as software on that physical TCA¨. The language used leaves room for misinterpretation and allows entities to use VM on physical TCA to bypass implementing security controls in the VM. VM image security should be verified prior to execution on TCA.

For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

3. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Disagree with adding R1.6 to CIP-005 as CIP-005 is written for protections of logical devices and data. This should be restored back to CIP-006 R1 Part 1.10.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.	
Likes 0	

Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern does not agree with the proposed change in Part 1.3. The way EACMS is written, it suggests that it includes all forms of EACMS and is too broad. The term “EACMS that enforce an ESP” is not bound to firewalls and switches with VLANs, in other words EACMS that enforce network segmentation. Domain Controllers for example can help “enforce” an ESP in determining who can and can’t cross the ESP. It is not clear, in that case, what the “Management Interface” of a domain controller EACMS is, nor can routable protocol be restricted to it if its used to authenticate users. The original approved standard lists Electronic Access Points for High and Medium BCS which more aligns with equipment within an ESP. Southern suggests considering the use of EAP as the object of this requirement to clarify the scope.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST believes modifications to CIP-005 should be limited to conforming changes only.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

There is insufficient clarity provided within the proposed terms to ensure consistent understanding and implementation of “Management Interface”. See response to #2 above.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA does not support the expansion of R1, Part 1.6 to include the protection of data traversing communications links. Expansion to communications links does not consider devices that cannot meet this criterion. Putting communication links in scope would increase costs and maintenance activities, and would require re-architecture of links. Additionally, Exemption 4.2.3.3 maintains the communications exemption for the equipment on the communications link in a ‘super-ESP’, whereas an encryption requirement when traversing multiple geographic locations would increase security for these super-ESPs. BPA suggests reverting to the Draft 3 language for R1, Part 1.6.

BPA does not agree with the requirement to mitigate risk represented by sharing memory resources in R2, Part 2.6.1. The theoretical risk represented by CPU-sharing is not high enough to mandate the significant re-architecture required to adequately separate CPU usage as specified in Part 2.6.1. BPA recommends allowing the continued use of shared resources to allow entities the flexibility to balance risk mitigation with resources, maintenance and cost of maintaining the grid.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC

Answer	No
Document Name	

Comment

CIP-005 R1.2 does not state that there must be a justification for the need of routable protocol communication except for in the Measures column.

We recommend the SDT change the wording from permit only needed routable protocol communications, and deny all other routable protocol communications “through the ESP” to “into identified ESP(s).”

ERC is defined as external routable ***connectivity***, but the requirement is for external routable ***communications***. This is another instance of the inconsistent use of routable protocol qualifiers.

In the Measures column of CIP-005 R1.2, the Measure “Physical isolation of an ESP,” is confusing.

The need to use routable “protocol” communications in the CIP-005 requirements is confusing. It makes it sound like routable ***protocol*** communications is something different than routable communications. You cannot have routable communications without a routable protocol unless you encapsulate the non-routable protocol. This current wording may support excluding serial communications that are encapsulated and transported via a routable protocol. It would be less ambiguous if the SDT drops the word “protocol” from routable protocol communications and just used “routable communications.”

For CIP-005 R1.5, we recommend the SDT add a “except during CIP Exceptional Circumstances” clause to the requirement (similar to the clause added to CIP-004 R3.5). There can be multiple single points of failure impacting the ability to detect known or suspected malicious IP communications. A logging server, line card, power source, management console or SIEM could fail resulting in an immediate potential instance of non-compliance. Many of these solutions require port mirroring and there are limitations to mirroring the same source networks to multiple destination interfaces. This creates a scenario where a failed patch or unexpected hardware failure would immediately result in a potential instance of non-compliance creating unnecessary administrative burden. One solution to solve this would be to use a SPAN aggregator that splits the SPANS to two different security devices (like an IDP), but this too creates a single point of failure that during a patch, reboot or any system failure, would automatically result in a potential instance of non-compliance.

For CIP-005 R2.1, the SDT should change the requirement so that the Interactive Remote Access is only initiated ***from*** an intermediate System instead of ***through*** an Intermediate System so that it’s clear that encrypted communication stops at the Intermediate System and new communication is then established from the Intermediate System.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	No
Document Name	

Comment

WEC Energy Group does not agree with the proposed edits in R1 as it references the new "Management Interface" definition of which we do not agree (see #2 response). We also note that the reference to the Electronic Access Point has been removed from the Applicable Systems column. The Electronic Access Point modified definition is suitable for referencing physical and virtual assets. Proposing the SDT leaves Electronic Access Point in the Applicable Systems column.

WEC Energy Group can support the proposed edits in R2 and R3.

Likes 0	
Dislikes 0	

Response

Kristine Martz - Amazon Web Services - 7

Answer	No
Document Name	

Comment

Regarding CIP-005 Part 1.4, AWS suggests not limiting authentication requirements to dial-up connections. The SDT should broaden this requirement to include other technologies (i.e. 4G, 5G, etc.). Limiting this requirement to dial-up only may inadvertently create a security gap where alternative connection methods are not required to authenticate.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

There is still a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication but have not enforced protections to ensure that malicious actors do not use the ports – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to the Standard to ensure validity of communications to Applicable Systems.

CIP-005-8 depends upon approved SCI terminology and other definitions associated with virtualization. Approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization.

There is a significant concern is that an entity could implement “logical isolation” using only a host-based firewall on essential systems that are directly connected to the internet. Thus, exposing them to greater risk as compared the requirements in place today using defense-in-depth.

Further, introducing Shared Cyber Infrastructure (SCI) increases the number of Requirements and Parts that a Responsible Entity needs to track compared to simply identifying the hypervisor and associated hardware and “high-water-marking” them with the highest identified impact rating and creating a BCS. Allowing “mixed-trust” environments within the same SCI (hypervisor) increases the complexity and management of the environment as the SDT relaxes the “high-water-marking” required to this point. In addition, complex environments are permitted where both ESP and non-ESP Cyber Assets can be commingled on the same hardware using nothing more than affinity rules and virtual networking to segregate these systems. The complexity surrounding these installations could allow for increased risks from configuration mistakes such that ESPs could contain Intermediate Systems.

Finally, there is no NERC definition of “Remediation VLAN” so therefore the Responsible Entity could keep VMs spun up and within the Remediation network for extended periods of time – without the benefit of protections from the other CIP Standards. Accidental connection to production networks before these VMs has been properly remediated could lead to security issues and introduction of malicious communications.

CIP-005 Requirement R1 Part 1.6 – to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters, does not carry a minimum level of encryption to be required. This could result in older less secure methods being used for connections leaving the data at risk. References to NIST documentation regarding minimum encryption is suggested. Further, dependence on third-party carriers to create the “super ESP” could allow encrypt-decrypt-encrypt situations that could jeopardize the required protections for confidentiality and integrity of the data.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3

Recommend update to Part 2.1. Remove “authorized” from “Permit authorized.”

Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not.

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3
Recommend update to Part 2.1. Remove “authorized” from “Permit authorized.”
Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not

Likes 0	
Dislikes 0	

Response

Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC

Answer	No
Document Name	

Comment

Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3

Recommend update to Part 2.1. Remove “authorized” from “Permit authorized.”

Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3

Recommend an update to Part 2.1. Remove “authorized” from “Permit authorized.”

Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3.

Recommend update to Part 2.1. Remove “authorized” from “Permit authorized.”

Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No
Document Name	2016-02_Virtualization_Unofficial_Comment_Form.docx

Comment

GSOC requests the SDT remove references to previous requirements regarding applicable systems and instead include the content in directly with regards to applicable systems in parts 2.2, 2.3, and 2.6.

In requirement 1.6, GSOC recommends allowing for the use of a combination of both physical and encryption controls at the discretion of the responsible entity for protections in the same manner as is allowed in CIP-012 standards. {C}[TK1]{C} This inclusion of physically security controls will provide more latitude for the entity to increase security while still remaining compliant rather than relying solely upon either physical or confidentiality and integrity controls. GSOC recommends using "Confidentiality and integrity controls, and/or", or an additional bullet point specifically allowing for a combination of confidentiality and integrity controls along with physical controls.

In requirement 2.1, specifying 'authorized IRA' implies that all IRA must be authorized, i.e. enumerated and documented. Additionally, the 2.1 measures then require all IRA be routed through an Intermediate System, suggesting even unauthorized IRA must do so as well. This issue persists in 2.3.

Requirement 2.5, 3.1, and 3.2 language on applicability should explicitly specify it applies to only SCI having vendor remote access, rather than every SCI.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)

Answer	No
Document Name	

Comment

The SRC suggests that IRA definition should remain unchanged and have the specific scenarios that these definition changes are attempting to address become part of the standard requirement language. (i.e. CIP-005-8 R2).

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	Yes

Document Name	
Comment	

Tri-State mostly agrees with the definition but thinks the second bullet,"Communication that originates from an Intermediate System"under what "IRA is not" is confusing. Isn't that system to system communication?

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS would like clarification on the restriction in R2.6.2. The part could be interpreted to restrict routable communication to any other devices or to restrict communication to those specific devices through an ESP.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying CIP-005 to allow for more flexibility in implementing future technologies while maintaining and even increasing security.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	
Comment	
PG&E supports the proposed modifications to CIP-005	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Manitoba Hydro agrees with the direction of the standard drafting team. Additional clarity could be added to sub-requirement R2.4 and R2.5. The term “with vendor remote access” has been added to the “applicable system” column. The addition of “SCI supporting an Applicable System in this Part” could mean that vendor remote access to the SCI is not in scope if there is no vendor remote access to BCS, since there are two qualifiers. Manitoba Hydro suggests adding a the qualifier “Where vendor remote access is implemented,” to the “requirements” column similar to the change done for R1.4 for Dial Up access.	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Chelan appreciates the SDT’s work on IRA and CIP-005 and approves the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	

Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the revisions made to CIP-005 in Draft #4.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment

EEI supports the revisions made to CIP-005 for Draft 4.

Likes 0	
Dislikes 0	

Response

William Steiner - Midwest Reliability Organization - 10

Answer	Yes
Document Name	

Comment

Part 1.5 – SCI is not afforded malicious communications protections like the other CA types. While we understand the desire to avoid monitoring heavy traffic like fiber-channel, there is still a real risk of malicious code over the network to/from hypervisors (and likely other SCI)

Part 1.6 – Communication between geographically dispersed SCI is not applicable, thus not necessarily afforded similar protections.

Part 1.6 - Including the 'Internet Protocol' qualification in the requirement could inhibit malicious communication detection for future technologies and implementations that may not use a traditional firewall and IP routing. In particular with the change from firewalls as the outer perimeter to a zero-trust implementation, there will likely be more configuration points that aren't also acting as routers, so the inherent protection from non-IP protocols offered by the separation of subnets will no longer be there and other protocols could pass.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

Cleco agrees with EEI comments.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
BC Hydro agrres with the proposed changes; however, clarification is needed as follows: In CIP-005-8 Requirement 2.1 which is, "Permit authorized....". The use of the word "authorized" is creating confusion. Typically IRA through the Intermediate System is already authorized through CIP-004. SCI was already added into CIP-004 scope therefore SCI access is authorized. IRA is applicable to all asset classifications on top of SCI which is also authorized through the CIP-004 process and not at the intermediate system. BC Hydro kindly requests that the drafting clarifies the use of the term "authorized" and recommends that the drafting team consider removing the word "authorized" from the wording of Requirement 2.1.	
Likes 0	
Dislikes 0	
Response	

Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Israel Perez - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE is concerned the definitions of Cyber Asset and PCA introduce security risks in CIP-005. The definition of Cyber Asset explicitly excludes SCI from its definition, which means SCI cannot be a Cyber Asset. The definition of PCA explicitly includes Cyber Assets or Virtual Cyber Assets in the definition. SCI cannot meet either definition, which means a hypervisor cannot be dual categorized as SCI and PCA. Therefore, an SCI placed within a network protected by an ESP arguably would not be subject to CIP-005 R1.1, R1.2, R1.5, or R1.6 despite being a PCA in all but definition.

In addition, Texas RE notes that SCI supporting high and medium impact BCS have fewer network-based protections than high and medium impact BCS. CIP-005 R1.2 is applicable to high and medium impact BCS with ERC. The requirement requires that only needed routable protocol communications are permitted through the ESP. CIP-005 R1.3 is applicable to SCI supporting medium and high impact BCS. The requirement requires that only needed routable protocol communications to and from the Management Interfaces are permitted.

Additionally, Texas RE is concerned there may be means of communicating with SCI outside of the narrow scope of the Management Interface definition. For example, an FTP server would not control the process of initializing, deploying, or configuring SCI. An FTP server is not an autonomous subsystem that provides access to the console independently of the host system’s CPU, firmware, or OS. Finally, an FTP server does not configure an ESP. As such, an FTP server running on SCI would be out of scope for CIP-005 R1.3. An FTP server in this scenario could be used to exfiltrate sensitive data, such as the disk images for the BCS that the SCI is hosting. Additionally, since SCI is out of scope for CIP-005 R1.5 entities would not be required to monitor this FTP server for malicious communications between the SCI and other systems. Texas RE suggests this issue would be mitigated by implementing high watermarking practices as described in Texas RE’s response in #9.

Lastly, Texas RE continues to be concerned the security objective for CIP-005-6 R1 Part 1.5 is now limited to IP malicious communications with the proposed changes. With the proposed changes this would not only reduce the compliance obligations but also create a gap in security by only focusing IP malicious communications versus all malicious communications.

Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	

4. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)

Answer	No
Document Name	

Comment

The SRC agrees with the concept of per system capability.

For Part 1.3, we recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible.

For Part 4.3, we request adding “security” to “applicable events” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”

For Part 4.4, please consider rewording this requirement to accommodate entities that use the current SIEM technology which has this type of functionality built-in and no longer requires a manual review of such data sources while also addressing those that do not have this technology.

For Part 5.1 and 5.4, leaving the scope of the term “system” up to the entity, requires effort to supply a definition and document compliance with the definition. This could lead to a misunderstanding of the intent of that term. We recommend that SDT update the technical rationale to include what is meant by “system”.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

No, 1.3 requirement is written more like measure with the word prevent. Would suggest rewording it to "Mitigate VCA's from CPU or memory vulnerabilities that share these resources with other VCA's that are not associated with the same impact categorization." Then prevention could be one of the measures.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
For Part 1.3, recommend changing “prevention” to “risk mitigation.”“Prevention” is absolute. “Risk mitigation” is flexible. Perhaps “prevention” can be moved to the Measures as a suggestion/ Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles. For Part 4.3, request adding “security” to “applicable event” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion. Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles. For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. The update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	

In R1.1, Ameren believes that the phrase "routable protocol network accessibility" is unclear and there should be more clarity as to what this phrase means. We are concerned an auditor might think of this phrase differently than Ameren does, so we believe more clarity around this phrase will ensure that auditors and Ameren have the same understanding as to what the phrase means.

In R4.3, the phrase "per system capability" was added. Does any paperwork need to be filled out and provided to the regional entity for devices that fall into the "per system capability" classification? For example, paperwork needs to be filled out for TFEs.

Likes 0	
Dislikes 0	

Response

Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC

Answer	No
Document Name	

Comment

For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion.

Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles.

For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion.
Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles.
For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion.

Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles.

For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”

Likes 0	
Dislikes 0	

Response

Ronald Bender - Nebraska Public Power District - 5

Answer	No
Document Name	

Comment

Recommend removing EACMS and PACS from the applicability section. If EACMS or PACS were to reside inside an ESP they are also categorized as PCAs so they will be covered. This change will exclude other CAs in a DMZ virtual system that do not perform EACMS or PACS functions and will thus retain the backward compatibility of the standard while allow greater protection for BCAs and PCAs.

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	No
Document Name	

Comment

Chelan believes the proposed language for CIP-007 R1.3 is overly burdensome and the required control does not reflect the actual risk of a VM escape attack. The intended controls (DRS affinity rules) listed in the measures are not intended for security control purposes, but are instead intended for resource control purposes. Because of this and the very broad applicability, they will have overly complex rulesets that introduce reliability risks where, in the event of a failure or during maintenance activities, a crucial VM may not be able to find a suitable host and crash. Given there are few if any demonstrated attacks along this threat axis, this seems to be an overreach.

Additionally, this requirement is not backwards compatible with the existing requirements. The currently effective requirements allow the mixing of EACMS and PACS VMs with out-of-scope VMs so long as the hosts themselves are classified as EACMS and PACS.

Finally, Chelan believes there is a Low Impact problem in the proposed requirement. The Applicable System is an SCI that hosts High or Medium Impact VCAs, not the actual High or Medium Impact VCAs themselves. The text of the requirement itself does not restrict itself to High and Medium and simply refers to “same impact classification”. If an SCI that hosts High or Medium Impact VCAs also hosts Low Impact BCS, the requirement is on the SCI to prevent sharing of CPU and memory between devices that are not of the same impact categorization, regardless of what that impact categorization might be. Low Impact is a different impact category from no impact, so the requirement would force the SCI to segregate Low Impact VCAs from no impact VCAs. That essentially places a requirement on Low Impact devices to not share CPU and memory with no-impact devices, so long as they are on the same SCI as a High and Medium impact VCA.

All that said, Chelan does recognize the risk of a zero day exploit along this vector and therefore, Chelan recommends this requirement should be restricted to BCAs and PCAs, and left EACMS and PACS out, which would be backwards compatible with the existing requirements and guidance. The suggested language below would prevent devices that are within the ESP from sharing CPU and memory with devices outside the ESP or in different impact level ESPs. This would accomplish the goal of protecting BES Cyber Systems and would simplify implementation by creating three categories of devices that may not share CPU and memory, rather than potentially six.

Chelan suggests the following language for CIP-007 R1.3:

Applicable Systems: SCI supporting: High Impact BCS and their associated PCA; Medium Impact BCS and their associated PCA

Requirement: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources, excluding storage resources, between High and Medium Impact BCS and their associated PCA, and VCAs that are not BCS or PCAs of the same impact categorization.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	No
Document Name	

Comment

WEC Energy Group does not agree with the proposed edits and retitling of R1. Changing the title of R1 to System Hardening implies the potential for more than just the management/monitoring of ports and services. Although "system hardening" is a best practice, it is at this time self defined and is too broad of a term to be used for CIP-007 R1 and in our opinion beyond the virtualization intent of the Project. Additionally, Part 1.1 implies ports and services in the Requirement, we understand it was rewritten in an attempt to address SCI supporting the Applicable System, however the rewrite is too broad and looses its intent of ports and services. Also note, the Measures for Part 1.1 describes the aspects of ports and services, why not use those same terms (ports and services) in the Requirement itself. Proposing the SDT leaves the title of the R1 as Ports and Services, leave R1 Part 1.1 and Part 1.2 as written and separate the SCI references included in current draft Part 1.3 into its own Requirment or Part.

WEC Energy Group can support the proposed edits in R2-R5.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

As it pertains to CIP-007 R4.2, the use of the term system in the statement “per system capability” leads to subjectivity. We recommend the use of “per Cyber Asset or BSC capability” as it defines the scope of capability.

Additionally, our comment from the last comment period of “If a firewall has VLANs on it for medium and low, or high and low, does that pull low impact network connection into scope because it shares the same firewall?” was not addressed by SDT as far as we know.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST believes modifications to CIP-007 should be limited to conforming changes only.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment	
Southern disagrees with the proposed changes to CIP-007 R1.3 Applicable Systems. Adding EACMS and PACS in both High and Medium Impact BCS increases the requirements for associated virtual assets. Southern agrees that for hypervisors which ALSO host BCS, the scope is appropriate, but for hypervisors that ONLY host EACMS outside of an ESP, with no BCS, it is an "anti-virtualization" incentive to dedicate hypervisors to a domain controller for example. Suggest changing the language to High/Medium Impact BCS and their associated PCA, which will keep this affinity requirement scoped to hypervisors that host BCS and anything else.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the revisions made to CIP-007 for Draft 4.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes

Document Name

Comment

AEP supports the revisions made to CIP-007 in Draft #4.

Likes 0

Dislikes 0

Response

Kimberly Turco - Constellation - 6

Answer Yes

Document Name

Comment

Kimberly Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer Yes

Document Name

Comment

Kimberly Turco, on behalf of Constellation Segments 5 and 6

Likes 0

Dislikes 0

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer Yes

Document Name

Comment

PG&E supports the proposed modifications to CIP-007.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying CIP-007 to allow for more flexibility in implementing future technologies while maintaining and even increasing security.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the revised CIP-007 proposed changes.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Magruder - Avista - Avista Corporation - 1

Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

“See comments submitted by the Edison Electric Institute”

Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE is concerned the language: “logical network accessible ports… including port ranges or services where needed to handle dynamic ports” was removed. Both ports and services are required to gain a better understanding of where vulnerabilities can exist whether in a physical or virtualized environment. Ports and services are often used for malicious reconnaissance and lateral movement within networks. Registered Entities should understand and document why ports and services are needed for many reasons (defense in depth, zero trust, etc. concepts).

Texas RE is concerned the phrase “CPU and memory resources” in CIP-007-7 Requirement R1.3 is written could be interpreted as (CPU and memory) resources or as CPU and (memory resources). Texas RE recommends rewording the sentence so it is clear that the CPU resources and memory resources should not be shared: “the sharing of CPU resources and memory resources.”

Additionally, in order to make the language of Requirement 1.3 more consistent with other requirements in CIP-007-7, Texas RE recommends revising the existing language Requirement R1.3 to “Prevent the sharing of CPU resources and memory resources, excluding storage resources, between Virtual Cyber Assets (VCAs) that are not of, or associated with, the same impact categorization.” The technical rationale for this requirement can then explain that the requirement is needed in order to mitigate the risk of CPU or memory vulnerabilities.

Lastly, Texas RE noticed inconsistent redlining between the “redline_to_last_approved” and “clean” copies of the standard for CIP-007-7 R4.1. In the “clean” version of the standards the following language, which Texas RE agrees with reads as:

Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events

In the “Redline to Last Approved” version the phrase “and after-the-fact investigations of” has been marked for removal. Texas RE does not agree with removing this phrase from the requirement.	
Likes 0	
Dislikes 0	
Response	

5. The SDT has used phrasing such as "SCI supporting an Applicable System from this Part" in the Applicable Systems column across many of the standards. Is it clear that this scopes the requirements for SCI to match the system(s) it hosts?

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA believes the phrase needs to be more specific. "Supporting" an Applicable System is too broad. BPA proposes adding SCI under the Applicable Systems column in the Requirements/Parts tables, grouping it with each appropriate impact rating similar to the way EACMS, PACS, and PCA are scoped. Additionally, the definitions for EACMS and PACS include SCI so these do not need to be accounted for. Alternatively, since the term "and their associated" is widely used in the standards, replacing the word supporting with "associated with" may be more clear.

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 6

Answer	No
Document Name	

Comment

The phrase "SCI supporting an Applicable System from this part" is still not clear enough and needs more verbage to explain what it applies to. The phrase could also be re-written as "SCI supporting the identified Applicable System in this Part"

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

"Part" is not a defined term, for additional clarity the drafting team could replace this phrase with "SCI supporting an Applicable System".

Lastly, "Applicable System" is used multiple times in the draft CIP standards and is not a defined term or a proposed defined term. The standard drafting team may consider defining this term in the NERC Glossary of Defined Terms.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

No, Supporting an applicable system is not specific enough and could be misterupted

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern agrees and appreciates the included language of “SCI supporting an Applicable System in this Part” across the many standards.

Likes 0	

Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees that the phrasing of “SCI supporting an Applicable System from this Part” is clear.	
Likes 0	
Dislikes 0	
Response	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy believes there is some lack of understanding at our company and throughout the industry on how SCI should be categorized when they are supporting EACMS or PACS and so, Xcel Energy supports the comments of the MRO NSRF. While Xcel Energy supports clarifications, our concerns do not rise to the level of requiring us to vote no on proposed Standards with SCI as an applicable system.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees the phrasing of “SCI supporting an Applicable System from this Part” in the Applicable Systems column in the Standards makes it clear the scoping is for the hosts the SCI supports.	
Likes 0	

Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
This is fairly clear. However it would be better to see some verbiage/examples in the technical rationale related to the inclusion of “storage resources required for system functionality of one or more Cyber Assets or VCAs….” found in the second bullet of the SCI definition to limit the scope of applicability. It’s not quite clear what exactly may be pulled into scope by the wording in the second bullet and there may be an unintentional increase in applicability. CIP-007 R1.3 specifically excludes storage resources in the requirement, but in the definition of SCI, the second bullet specifically includes storage resources in the definition of SCI.	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes

Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the phrasing “SCI supporting an Applicable System from this Part” in the Applicable Systems column across many of the standards is clear.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	

Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennifer Wright - Sempra - San Diego Gas and Electric - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

patricia ireland - DTE Energy - 4, Group Name DTE Energy

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer	
Document Name	

Comment

“See comments submitted by the Edison Electric Institute”

Likes 0	
Dislikes 0	

Response

6. The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Alliant Energy supports the comments submitted by the MRO NSRF

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	CIP-010 Alternate Update.docx

Comment

ecommending maintaining the CIP-010-4 requirement to establish and maintain the baseline.

Justification:

While the TR does allude to the use of the baseline configuration as the “how” this requirement can be met, it is followed by stating the entity would be required to document how the baseline meets the stated security objective and references NIST SP 800-128 as a guide.

Throughout NIST SP 800-128 the baseline configuration is referenced as the “secure state”, specifically “…*baseline configuration for a system and associated components represents the most secure state consistent with operational requirements and constraints*” (NIST.SP.800-128, Section 2.2.2, pp. 21). Establishment and maintenance of a baseline configuration provides the entity with a secure starting point from which each modification can build upon.

Removing the requirement for a baseline configuration and/or requiring the entity to justify the use of the baseline appears to go against the guidance provided in NIST 800-128.

R1 Response

Part 1.1

R1.1 Document and maintain system configurations (to include at a minimum software addressing the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.)

R1.1.1 Manage changes which alter the system configuration

R1.1.2 Authorize changes to the system configuration

R1.1.3 Validate implementation of changes to the system configuration

Part 1.2

1.2.1. Prior to implementing a change to system configurations from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 andCIP-007 remain implemented as required; and

1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Part 1.3

For a change that deviates from the existing system configuration, update the system configuration documentation as necessary within 30 calendar days of completing the change.

R2 – Security Configuration Monitoring

Considering the changes made to R1 and the proposal to maintain the baseline configuration documentation requirements the following is a proposed adjustment to R1.

Response

Part 2.1

Methods to monitor at least once every 35 calendar days for unauthorized changes to the system configuration. Document and investigate detected unauthorized changes.

1 – The language used in the requirement, specifically “settings”, will force a significant and increasing administrative burden on the Entities. The control which applies to the requirement for each of the items within CIP-005 and CIP-007 will typically contain a multitude of “settings” which enforces the configuration of the control as a collective. There is a concern that the Entity will be ‘too far in the weeds’ focusing on the numerous settings that contribute to a control thereby diverting attention from the security posture of the environment.

2 – Confirmation after implementation of the authorized/documented change of the controls which enforces the requirement in CIP-005 and CIP-007 ensures the security configuration of the applicable system was not impacted in a manner that would weaken the security posture of the applicable system.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)

Answer	No

Document Name

Comment

The proposed changes to CIP-010 are SRC’s gravest concern as we believe the proposed changes go beyond what was previously in the CIP standards such that they would no longer be backwards compatible. In particular, the addition of the concept of “settings changes” is overly broad; whereas the prior standard focused on changes to the baseline configuration. SRC proposes “settings changes” be modified to “configuration changes” or eliminated altogether.

For consistency, please add the term “Cyber” to security patches.

The SRC requests clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document that baselines (from previously approved Standard) track or show any changes made to applicable CIP-005 and CIP-007 security controls

The SRC requests that consistent language be used when addressing the same subject in different parts of the standard within the Requirements of Parts 1.1 and 1.3. Examples of this include the following:

- *Part 1.1 provides what is included in software*
- *Part 1.3 distinguishes some of 1.1 apart from software*
- *Part 1.1 starts with “Control the implementation of intended changes to software, or intended changes to settings . . .”*
- *Part 1.1 also says “Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.*
- *Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .”*

While we recommend that that CIP-010 R1 needs to be left “as is” as changing the requirement may present a greater compliance burden on the entity with a less clear objective/goal. The proposed changes do not increase the level of security that are currently afforded by the existing standard.

For Part 2.1, we recommend this requirement is also left “as is”. The proposed requirement is overly burdensome and may require the monitoring of the entire asset, including its filesystem, registry, miscellaneous settings, accounts, etc. and is above and beyond what is currently required with little added security benefit.

Likes 0

Dislikes 0

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer No

Document Name

Comment

R1.1 The phrase "...could weaken configured cyber security controls.." is very general and expands the original baseline scope widely to include endless settings that could be under the review of an audit.

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	CIP-010 Alternate Update.docx

Comment

Recommending maintaining the CIP-010-4 requirement to establish and maintain the baseline.

Justification:

While the TR does allude to the use of the baseline configuration as the “how” this requirement can be met, it is followed by stating the entity would be required to document how the baseline meets the stated security objective and references NIST SP 800-128 as a guide.

Throughout NIST SP 800-128 the baseline configuration is referenced as the “secure state”, specifically “…*baseline configuration for a system and associated components represents the most secure state consistent with operational requirements and constraints*” (NIST.SP.800-128, Section 2.2.2, pp. 21). Establishment and maintenance of a baseline configuration provides the entity with a secure starting point from which each modification can build upon.

Removing the requirement for a baseline configuration and/or requiring the entity to justify the use of the baseline appears to go against the guidance provided in NIST 800-128.

R1 Response

Part 1.1

R1.1 Document and maintain system configurations (to include at a minimum software addressing the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.)

R1.1.1 Manage changes which alter the system configuration

R1.1.2 Authorize changes to the system configuration

R1.1.3 Validate implementation of changes to the system configuration

Part 1.2

1.2.1. Prior to implementing a change to system configurations from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 andCIP-007 remain implemented as required; and

1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Part 1.3

For a change that deviates from the existing system configuration, update the system configuration documentation as necessary within 30 calendar days of completing the change.

R2 – Security Configuration Monitoring

Considering the changes made to R1 and the proposal to maintain the baseline configuration documentation requirements the following is a proposed adjustment to R1.

Response

Part 2.1

Methods to monitor at least once every 35 calendar days for unauthorized changes to the system configuration. Document and investigate detected unauthorized changes.

1 – The language used in the requirement, specifically "settings", will force a significant and increasing administrative burden on the Entities. The control which applies to the requirement for each of the items within CIP-005 and CIP-007 will typically contain a multitude of "settings" which enforces the configuration of the control as a collective. There is a concern that the Entity will be 'too far in the weeds' focusing on the numerous settings that contribute to a control thereby diverting attention from the security posture of the environment.

2 – Confirmation after implementation of the authorized/documented change of the controls which enforces the requirement in CIP-005 and CIP-007 ensures the security configuration of the applicable system was not impacted in a manner that would weaken the security posture of the applicable system.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

R1.3 – consistency of phrases among the requirements is necessary, For instance, in Requirement 1 part 3, the phrase used is "Prior to installation." In other sections, however, the phrase used is "prior to the intended change" One of the two phrases should be used throughout.

Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls.

Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with "Control the implementation of intended changes to software, or intended changes to settings . . ." Part 1.1 also says "Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches." Part 1.3 starts with "Prior to the installation of operating systems, firmware, software, or software patches . . ."

For Part 3.3, request clarification on the first Requirement bullet – "Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System." The term "like replacement" is an undefined term. Does the SDT intend for the entity to define this term? "Configuration of the previous" implies a baseline that was not specified. As written, the entity's interpretation may be different than the auditor's.

For Part 3.3, request removing "any" from the first Measures bullet because "any" is a scope concern where "any" is interpreted as "all."

For 1.3 in Attachment 1, recommend changing this new bullet from "Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;" to "provide valid mitigation" since there may be newer software vulnerabilities that the earlier state has not addressed.

Likes 0	
Dislikes 0	

Response

Jennifer Wright - Sempra - San Diego Gas and Electric - 5

Answer	No
Document Name	

Comment

The word "setting" should be further clarified.

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

SPP would like to understand how the significant proposed changes in CIP-010-5, specifically Requirement R1, relate to what was requested in the Project 2016-02 SAR. SPP believes that the verbiage related to SCI, containerization, and ESPs between systems with different impact ratings can be added without having to change the way that entities have to comply with CIP-010 today.

The new proposed language greatly expands the scope for CIP-010 and raises concerns for backwards compatibility with existing baseline methods, adds unnecessary complexity, and significantly increases cost with minimal security benefit. The current baseline configuration

requirements have been moved to the Measures column along with additional verbiage to address virtualization. However, the control language is very broad and can lead to different interpretations depending on the auditor and uncertainty in tracking changes. Responsible Entities have demonstrated that both physical and virtual systems are capable of developing, documenting, approving, tracking, updating, and monitoring baseline configurations. For these reasons, SPP believes that the prescribed baseline configuration requirements should remain in place with the addition of specific verbiage related to virtual architecture and containerization. The baseline language supports a secure baseline configuration and represents industry best security practices.

The NIST 800-128 guidelines refer to applying the security configuration management practices that include "monitoring the configuration of systems to ensure that configurations are not inadvertently altered from the approved baseline", thus implying that baseline configuration management is key to securing a system. These guidelines further define a Baseline Configuration as, "A set of specifications for a system, or CI within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes." This definition fits well with the currently approved verbiage in CIP-010-4 where the "set of specifications for a system" was clearly defined for the baseline and approved through change control methods. The baseline is an understanding of what the approved system configuration should be so that there is an understanding of what has changed. According to NIST, the baseline configuration should represent a secure state of the system while also maintaining a "cost-effective and functional support of mission and business processes". The updated control verbiage does not reference a baseline configuration and does not adhere to a cost-effective support of security best practices, therefore creating a risk to demonstrate compliance.

The following proposed language for CIP-010-5, Requirement R1, Part 1.1, could address virtualization while also maximizing backwards compatibility:

Develop a baseline configuration, individually or by group, which shall include the following items:

1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;

1.1.2. Any commercially available or open-source application software (including version)

intentionally installed including application containers;

1.1.3. Any custom software installed, including application containers;

1.1.4. Configuration that modifies network accessible logical ports or network accessible services on an Applicable System;

1.1.5. Any security patches applied;

1.1.6. SCI configuration of host affinity control between systems with different impact ratings;

1.1.7. Changes to configurations or settings for an ESP between systems with different impact ratings; and

1.1.8. Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	No
Document Name	

Comment

While we appreciate the thoughtful proposal of a less prescriptive requirement for CIP-010, there are many unintended consequences with the expansion of scope in the currently proposed language. The word “settings” scopes too many possible features into CIP-010 that do not necessarily have a compelling security value. Additionally, the concept of a baseline is foundational in NIST SP 800-128 . It is possible to have less prescriptive requirements that advance the intention of CIP-010 and its security objectives,while maintaining true backward compatiability.Here is our alternate proposal that we have worked with Exelon to craft:

R1.1 Document and maintain system configurations (to include at a minimum software addressing the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.)

R1.1.1 Manage changes which alter the system configuration

R1.1.2 Authorize changes to the system configuration

R1.1.3 Validate implementation of changes to the system configuration

R1.2.1. Prior to implementing a change to system configurations from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 andCIP-007 remain implemented as required; and

R1.2.2. Document the results of the testing, and if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

R1.3 For a change that deviates from the existing system configuration, update the system configuration documentation as necessary within 30 calendar days of completing the change.

R2.1 Methods to monitor at least once every 35 calendar days for unauthorized changes to the system configuration. Document and investigate detected unauthorized changes.

Likes 0	

Dislikes 0

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer No

Document Name

Comment

Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. The entity may need to document its baselines (from previously approved standards) when addressing its CIP-005 and CIP-007 security controls.

Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in the software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to the software or intended changes to settings . . .” Part 1.1 also says “Changes to the software include the installation, removal, or update of the operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .”

For Part 3.3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term? “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s.

For Part 3.3, request removing “any” from the first Measures bullet because any is a scope concern . . . where any is interpreted as “all.”

For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.

Likes 0

Dislikes 0

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer No

Document Name

Comment

BC Hydro appreciates the opportunity to review and offers the following comments:

1. CIP-007 and CIP-005 Standards were modified to explicitly call out specific controls related to SCI (e.g. CIP-007 R1.3 / CIP-005 R1.3) but in CIP-010 R1 it is not written with the same clarity. For example, in CIP-010-3 R1.1 measures provided are not truly applicable to non SCI CIP-007 and CIP-005 controls. Operationally they differ greatly from non-SCI classified assets. Similar to the pattern followed in CIP-005 and CIP-007 changes, BC Hydro proposes to call out in a separate requirement SCI controls that need to be evaluated.

2. The inclusion of the following "... or intended changes to settings that could weaken configured cyber security controls required by CIP005 and CIP-007" makes the Requirement R1.1 of CIP-010-3 unclear. It is indicative that this Requirement will only apply if the change in settings has an effect on the configured CIP-007 and CIP-005 controls. However the expected scope of changes in settings need clear direction and guidance. Some pertinent use case examples and clear direction is needed here.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

Ameren believes that R1.1 is too large of a requirement and should be split up into multiple smaller requirements.

In R2.1, Ameren would like examples of "settings that could weaken configured cyber security controls," because this could be left up to interpretation.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	No
Document Name	

Comment

Cleco agrees with EEI comments.

Likes 0	
Dislikes 0	

Response

Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo

Answer	No
Document Name	

Comment

Concerns regarding backward compatibility. And how compliance on existing practices will be assessed following the proposed change. Specifically how current practices related to “Live operating system and software executable only from read-only Media” can still need the intent of Section 1.3 without subjectivity inherent in the “other mitigation methods” option. Request adding of technical rationale (i.e. the intent of the change) for Attachment 1 Section 1.3. in particular explanation on the bullet that was added, i.e. “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution”.

Support comment from NPCC RSC. Reiterated here: “For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.”

Likes 0

Dislikes 0

Response

Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC

Answer No

Document Name

Comment

For requirement 1.1.2, we suggest to simply write, “Verify the required cyber security controls remain implemented”. There is confusion as to why “…as required as a part of the change” adds to the requirement.

However, the newest version is closer to what is done by industries. Old version address the case when a plan made its own programs in assembly language. Now, it’s more representative of the real world when third-party software executables are buy and install in systems.

1) It is unclear if Management Interface of Cyber System is in scope for CIP-010

Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document that their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls.

Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to software, or intended changes to settings . . .” Part 1.1 also says “Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .”

For Part 3,3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term. “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s.

For Part 3.3, request removing “any” from the first Measures bullet because any is a scope concern . . . where any is interpreted as “all.”

For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls.
Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to software, or intended changes to settings . . .” Part 1.1 also says “Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .”
For Part 3.3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term. “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s.
For Part 3.3, request removing “any” from the first Measures bullet because any is a scope concern . . . where any is interpreted as “all.”
For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

For requirement 1.1.2, we suggest to simply write, “Verify the required cyber security controls remain implemented”. There is confusion as to why “…as required as a part of the change” adds to the requirement.

However, the newest version is closer to what is done by industries. Old version address the case when a plan made its own programs in assembly language. Now, it’s more representative of the real world when third-party software executables are buy and install in systems.

{C}1) It is unclear if Management Interface of Cyber System is in scope for CIP-010

{C}2) The usage of ¨OR¨ seems to allow entities not to control changes to software. Suggest using the ¨AND¨ instead in ¨Control the implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007¨

Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document that their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls.

Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to software, or intended changes to settings . . .” Part 1.1 also says “Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .”

For Part 3,3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term. “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s.

For Part 3.3, request removing “any” from the first Measures bullet because any is a scope concern . . . where any is interpreted as “all.”

For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.

Likes 0	
Dislikes 0	

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

In the proposed language, the term “could weaken” as it applies to changes requiring configuration management controls is vague and, as undefined, leaves the determination unsupported by existing definitions. GSOC suggests either substituting “alters” or adding “ . . . as determined by the responsible entity”. As proposed, change management controls would only need to be utilized for a type of change that undermines existing security and not for all changes.

Additionally, as proposed, the language of 1.1.2 could subject the responsible entity to double jeopardy violationof CIP-010 as well as the underlying violations of CIP-005 and CIP-007.. Additionally, as written, every control must be reviewed for every applicable change regardless of whether it is technical, procedural, or impacted by the change. GSOC recommends the removal of 1.1.2 as a separate requirement and inclusion in measures.

Likes 0	
Dislikes 0	

Response

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP appreciates SDT’s efforts in making requirements more clear. However, AEP does not support R1.2 and R2.1 and states recommendations below.

- **R 1.2.1**: SDT added **“the configuration of”** as in “…where the test is performed in a manner that minimizes adverse effects to ensure **that the configuration of** required cyber security controls in CIP-005 and CIP-007 reamin implemented as required”. AEP suggests removing this added language as it is too prescriptive.
- **R2.1**: AEP questions the statement "*unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007*" and recommend SDT to revert the requirement languages as proposed in Draft #3, i.e., “Methods to monitor for unauthorized changes at least once every 35 calendar days. Document and investigate detected unauthorized changes.”.

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	No
Document Name	

Comment

Constellation supports comments that were submitted by Exelon Corporation.

Kimberly Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Alison Mackellar - Constellation - 5

Answer	No
Document Name	

Comment	
Constellation supports comments that were submitted by Exelon Corporation. Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the comments written in the EEI response	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
R1-Removing baseline configuration does not change what needs to be done in practice. Entities will still need to retain a baseline configuration as evidence from which to establish the changes that were authorized. · For Part 1.1 an entity will still need to show the baseline configuration prior to the change to show required cyber security controls in CIP-005 and CIP-007 are not adversely affected. · For Part 2.1 an entity will still need to provide baseline configurations for evidence that they monitor at least once every 35 calendar days for unauthorized changes to the items listed Parts 1.1 and 1.2. For R3-the concern is that Remediation VLANs should be properly defined in the technical rational or Glossary as it may introduce situations where an entity could inadvertently place production Cyber Assets in this VLAN.	
Likes 0	

Dislikes 0

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	No
Document Name	

Comment

In large part, the proposed changes are fine. However, there is an implication by virtue of the new veribiage and removal of “baseline configurations” that additional configuration items (outside of the original “baseline configuration”) need to be included within change management. Such additional configuration items are not explicitly included in the Measures section, thus leaving this aspect of the requirement wholly subjective. Additionally, the third bullet on slide 39 from the Project 2016-02 Webinar seems to implicitly add a documentation requirement for the analysis/comparison of baseline configurations to security controls. This ask is not in the requirement. Including it in the Webinar presentation empowers Regional auditors to ask for evidence of requirements that are not included in the standard or measures sections.

Likes 0

Dislikes 0

Response

Kristine Martz - Amazon Web Services - 7

Answer	No
Document Name	

Comment

AWS agrees with changes to CIP-010 R1, R2, and R3. However, AWS remains concerned that CIP-010 R4 does not address security risks associated with virtual machines (VM) hosted on physical Transient Cyber Assets (TCAs) because the standard language states that a VM running on a physical TCA can be treated as software. We acknowledge the SDT response to the previous comments in the consideration of comments, but we still see security risks and have provided our previous comment below for context.

The Standard allows an entity to choose one or a combination of security controls that may not extend cyber security protections to the VM itself leaving VMs potentially vulnerable to security threats undetected by the physical host. We propose removing the language “Virtual machines hosted on a physical TCA can be treated as software on that physical TCA” from the TCA definition. By removing this language, entities would be required to apply security controls to the virtual machines hosted on their physical TCAs in alignment with CIP-010 R4.

Likes 0

Dislikes 0

Response

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	

The current phrasing of Part 1.1.2 implies that entities must verify all “required cyber security controls remain implemented as required” for any change to software or security settings even if the change itself does not impact a certain control (e.g. a windows patch typically doesn’t modify an ESP/EAP for CIP-005, updating a FW Policy does not impact CIP-007 R2, etc.). This new language removes entities abilities to identify potential impacts and verify/test those impacts as allowed by the in-effect standard and the previous revision. Entergy is concerned that this language as written would require entities an undue burden to re-verify non-impacted controls for every change. While the Measures section implies that an entity has latitude to identify which cyber security controls should be verified (“ a list of cyber security controls verified”) this is not clearly aligned with the language of the standard.

Entergy recommends adding clarifying language to CIP-010 R1 Part 1.1 that entities verify potentially impacted cyber security controls, such as “Verify the required cyber security controls ***identified by the Responsible Entity that could be weakened*** remain implemented as required as part of the change.” This would allow entities to focus verification efforts on potentially impacted controls based on the nature of the change, instead of a one-size fits all approach of re-verifying every CIP-005 and CIP-007 control for every change.

Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	

In large part, the proposed changes are fine. However, there is an implication by virtue of the new veribiage and removal of “baseline configurations” that additional configuration items (outside of the original “baseline configuration”) need to be included within change management. Such additional configuration items are not explicitly included in the Measures section, thus leaving this aspect of the requirement wholly subjective. Additionally, the third bullet on slide 39 from the Project 2016-02 Webinar seems to implicitly add a documentation requirement for the analysis/comparison of baseline configurations to security controls. This ask is not in the requirement. Including it in the Webinar presentation empowers Regional auditors to ask for evidence of requirements that are not included in the standard or measures sections.

Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No

Document Name	

Comment

CIP-010 R2.1 as written would require an audit of every setting that could impact a CIP-005 or CIP-007 security control every 35 calendar days on High Impact devices. For some devices, this could be hundreds of individual settings, and Cyber Assets may not provide these settings in a way that audit of those settings could be automated. This would also effectively be a baseline configuration, though a more rigorous one than required by the currently effective requirements, as each setting would have a “baseline” to ensure the effectiveness of the security control it implements.

Chelan finds it difficult to develop a requirement that accomplishes the same security objective CIP-010 R2.1 of auditing that unauthorized changes have not occurred without the development of a baseline configuration to compare against. By definition, auditing changes requires you to have a known good state, essentially a baseline configuration. If the SDT wishes to eliminate baseline configurations, it should eliminate the periodic monitoring for unauthorized changes, or change the security objective.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	No
Document Name	

Comment

Similar to the MRO-NSRFs response, WEC Energy Group wishes to bring attention to the added phrase in CIP-010 Requirement 1 Part R1.1, “…or intended changes to settings that could weaken configured cyber security controls required by CIP005 and CIP-007.” We also would raise concerns with the current proposed Measures for R1.1.

This language raises questions. On applicable systems, are entities expected to authorize/monitor for both software changes AND settings that could weaken cyber security controls. Or does the ‘or’ indicate that choosing one of those would fulfill the obligations? For instance, consider a password change on a service account/agent which unintentionally breaks logging capabilities on an unspecified BCA. While an entity would be in violation of CIP-007 R4, with this new CIP-010 language, would the password change constitute a “change to settings” which weakened a CIP-007 control (R4.2) and therefore have been required to navigate the change management process? Would simply changing an applicable password from 10 characters to 9 characters constitute a weakening of CIP-005/CIP-007 cyber security controls?

There are many configuration changes that currently don’t affect one of the baseline items but could be considered in scope in the new version of the standard (for example, modification of anti-virus settings or any configuration settings on a firewall). This addition, combined with one of the statements made during the September 12, 2022 webinar that entities may have more compliance work to perform under the revised CIP-010, indicates that the scope of change management is broadened under the proposed revisions. This directly contradicts other statements that have stressed how the revisions are to be backwards compatible. The idea being that any entity that is in compliance today with current technologies and processes will be compliant under the revised standards, even if they do not seek to employ or utilize virtualization technologies.

We recommend the SDT to revisit the proposed CIP-010 R1.1 language and undertake any further revision needed to ensure that the scope of CIP-010 R1 is not expanded any more than necessary. One recommendation would be to separate both R1.1 into two parts, one addressing BCAs only, which would mirror existing CIP-010-3 R1.1 language, and one addressing SCI specifically which would further clarify “settings” (this would also necessitate splitting the proposed R2.1 into two different requirements as well).

Secondly, it seems that there continues to be confusion in the industry over whether or not to baseline and what are the best methods by which to demonstrate compliance with CIP-010 R1.1. We note that, while the Measures for R1.1 are quite lengthy, all the detail is about what the “documented process" should address or include, without suggesting examples of what the documented process could actually be documented as. We approve of providing options for entities to comply with CIP-010 R1.1 without necessarily having to maintain and demonstrate a documented baseline but it's also true that many utilities wish to continue using precisely that approach for their compliance – yet the word baseline is missing entirely from the Measures section of CIP-010 R1.1. We understand that "documented process" that includes the various items listed implies a baseline, but there is no reason we see not to just then come out and say "baseline" is an example of an acceptable option.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC

Answer	No
Document Name	

Comment

The new proposed wording is challenging to navigate and subjective. For example, what does it mean to weaken the configured cybersecurity controls and settings?

We recommend changing CIP-010 R1.1 back to the previous wording, and restore previous requirement parts through R2.1, and add "SCI supporting an Applicable System in this Part". This change is out of scope to support virtualization other than adding SCI to the applicability column. The proposed changes do nothing to support virtualization but do add significant ambiguity to the requirement. Also, a baseline MUST be established if there is going to be a requirement to monitor for unauthorized changes.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The MRO NSRF wish to bring attention to the added phrase in CIP-010 Requirement 1 Part R1.1, "…or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007." The MRO NSRF also would raise concerns with the current proposed Measures for R1.1.

This language raises questions. On applicable systems, are entities expected to authorize/monitor for both software changes AND settings that could weaken cyber security controls. or does the 'or' indicate that choosing one of those would fulfill the obligations? For instance, consider a password change on a service account/agent which unintentionally breaks logging capabilities on an unspecified BCA. While an entity would be in violation of CIP-007 R4, with this new CIP-010 language, would the password change constitute a "change to settings" which weakened a CIP-007 control (R4.2)

and therefore have been required to navigate the change management process? Would simply changing an applicable password from 10 characters to 9 characters constitute a weakening of CIP-005/CIP-007 cyber security controls?
There are many configuration changes that currently don't affect one of the baseline items but could be considered in scope in the new version of the standard (for example, modification of anti-virus settings or any configuration settings on a firewall). This addition, combined with one of the statements made during the September 12, 2022 webinar that entities may have more compliance work to perform under the revised CIP-010, indicates that the scope of change management is broadened under the proposed revisions. This flies in the face of other statements that have stressed how the revisions are to be backwards compatible and that any entity that is in compliance today with current technologies and processes will be compliant under the revised standards even if they do not seek to employ or utilize virtualization technologies.

Secondly, it seems that there continues to be confusion in the industry over whether or not to baseline and what are the best methods by which to demonstrate compliance with CIP-010 R1.1. The MRO NSRF note that, while the Measures for R1.1 are quite lengthy, all the detail is about what the "documented process" should address or include, without suggesting examples of what the documented process could actually be documented as. The MRO NSRF approve of providing options for entities to comply with CIP-010 R1.1 without necessarily having to maintain and demonstrate a documented baseline but it's also true that many utilities wish to continue using precisely that approach for their compliance – yet the word baseline is missing entirely from the Measures section of CIP-010 R1.1. The MRO NSRF understand that "documented process" that includes the various items listed implies a baseline, but there is no reason the MRO NSRF see not to just then come out and say "baseline" is an example of an acceptable option.

The MRO NSRF recommend that the first paragraph of R1.1 Requirement be rewritten to read, "Control the implementation of intended changes to Applicable Systems that could weaken configured cyber security controls required by CIP-005 and CIP-007." The MRO NSRF also recommend the inclusion of the word "baseline" as an example in the R1.1 Measures of a type of documented process that Registered Entities may employ to demonstrate their compliance with R1.1. Alternatively, if this recommendation is not acceptable, then some other change in verbiage that provides Entities the option of either continuing to comply using current baseline and baseline deviation tracking methods, or allowing a different approach per the new requirement and measure language, to ensure for the allowance of backward compatibility.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

In Measures to revised R1.1.2, the only example given of a tool used to verify required security controls [required by CIP-005 and CIP-007] remain implemented is a vulnerability scanner. It is unlikely that this will be the tool used to verify these controls, and that guidance may be misleading to Regional Entity auditors. It is more likely that a configuration management database will be used to verify that software is installed and that controls such as listening ports, disabled accounts, password controls, antimalware settings, and applied security patches are unchanged. CEHE recommends that the SDT add "configuration management database" as an example in the Measures in R1.1.2.

In R3.3, the exception for replacement of the same type of Cyber System with a configuration of the previous or other existing Cyber System should be revised to include additions of the same type, not only replacements. An example is adding a console from an identical known good image as existing consoles. This is not a replacement, but from a security and reliability perspective, has the same effect. Language should be revised to say "Like replacements or additions of the same type of Cyber System with a configuration of the previous or other existing Cyber System".

Likes 0	
Dislikes 0	

Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
In Measures to revised R1.1.2, the only example given of a tool used to verify required security controls [required by CIP-005 and CIP-007] remain implemented is a vulnerability scanner. It is unlikely that this will be the tool used to verify these controls, and that guidance may be misleading to Regional Entity auditors. It is more likely that a configuration management database will be used to verify that software is installed and that controls such as listening ports, disabled accounts, password controls, antimalware settings, and applied security patches are unchanged. SIGE recommends that the SDT add “configuration management database” as an example in the Measures in R1.1.2. In R3.3, the exception for replacement of the same type of Cyber System with a configuration of the previous or other existing Cyber System should be revised to include additions of the same type, not only replacements. An example is adding a console from an identical known good image as existing consoles. This is not a replacement, but from a security and reliability perspective, has the same effect. Language should be revised to say “Like replacements or additions of the same type of Cyber System with a configuration of the previous or other existing Cyber System”.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
For R2 Dominion Energy recommends reverting back to the previous language and include verbiage excluding password changes. The term “settings” is too subjective and can be interpreted inconsistently. Additionally, for the Severity Level for R1, Dominion believes the SAR was intended to address virtualization and arbitrarily changing the VSL for R1 is not in scope. Dominion recommends reverting back to the previous language	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 6	
Answer	No

Document Name

Comment

We still have concerns on CIP-010-5 because the draft does not include the Guidelines and Technical Basis section where it defines what must be included in a vulnerability assessment. It is understood that the Standards Drafting team emphasizes backwards compatibility, but, the proposed changes to CIP-007 R1 and CIP-010 R1.1 could affect what is required in the vulnerability assessments. At the very least, we would like to know and comment on what additional items will be required for SCI in a vulnerability assessment as there is nothing found in the current proposed changes.

Lastly, under CIP-010 R3.3 BES Cyber System is shortened to BCS. However, this is different than the other parts of CIP-010 R3. We recommend consistency.

Likes 0

Dislikes 0

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer No

Document Name

Comment

NST believes modifications to CIP-010 should be limited to conforming changes only.

Likes 0

Dislikes 0

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer No

Document Name

Comment

Southern disagrees with Part 1.1 Requirements that includes the phrase “settings that could weaken cyber security controls required by CIP-005 and CIP-007”. Southern finds this phrase overly broad, questioning if full compliance could ever be proven out of the universe of “settings” (registry settings, configuration paramenters, per application settings, etc.). Added to the complexity of knowing all settings is the phrase “could weaken” adding in the idea of ‘potential’ to this already elusive scope. Southern suggests the SDT reconsider the concept used in draft 3 of the entity defining the higher level types of changes they have in their change management programs. In addition, to provide further clarity of scope, Southern suggests the SDT go through CIP-005 and CIP-007 and list the areas that should be under CIP-010 change management. Since these requirements are the same for every entity, that list should be the same for every entity.

Likes 0

Dislikes 0

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

The language "…changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007" is subjective. There could be any number of "settings" that "could weaken" the security controls. Can guidance be given such as some exapmples of these settings that could be used to weaken the security controls? Also, is "software patches" synonymous with "security patches" or are these two (2) different entities of their own?

Likes 0

Dislikes 0

Response

Jodirah Green - ACES Power Marketing - 6

Answer	Yes
Document Name	

Comment

We feel using "could" in parts of CIP-010-5 is very subjective and is not necessary. Further the measures uses "may" instead of "could". A change either does or doesn't affect cybersecurity controls required by CIP-005 and CIP-007. We are fine with the language, but feel it would be cleaner and less ambiguous without "could".

Likes 0

Dislikes 0

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the revisions made to CIP-010 for Draft 4.

Likes 0	
Dislikes 0	

Response

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6

Answer	Yes
Document Name	

Comment

NEE requests the SDT apply linkages in CIP-010-5 R1 P1.1 to all subparts for software scope. Suggest clarity that all subparts refer back to the software scope definition established in CIP-010-5 R1 P1.1.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
Document Name	

Comment

MPC supports comments that were submitted by the MRO NERC Standards Review Forum.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E supports the modification made to CIP-010, but PG&E provides the following recommendation:

The text of "…intended changes to settings …" withing the Requirement language be clarified to avoid un-intended consequence of setting changes that would not have an impact on the CIP-005 and CIP-007 controls from being brought into scope of Audit Teams.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

NV Energy supports the revisions for CIP-010-5, but harbors some concern regarding unclear language in Requirement R1, subpart 1.1. The word "settings" does not enjoy the same clarifying language as does the word "software". We believe this creates a risk for unpredicatble interpretation without any additional technical rationale defining the intent of the word. NV Energy suggests "settings" receive a definition complementary to "software" to better assist entities reach compliance, but ultimately feels the language in its current state is workable although not ideal.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed changes to CIP-010 but feel the following "weaken" statement introduced in part R1.1, without an official definition, leads to uncertainty and lack of clarity around the items that may fall into change management. This will result in re-examination of existing systems and baselining methodologies that threaten the intended backwards compatibility of the new requirements. In addition, we agree with EEI stance that which "settings" are in scope requires additional clarification.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes

Document Name	
Comment	
BPA believes CIP-010 R2.1 needs a verb in front of beginning of the Requirement language.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE continues to be concerned security obligations will be reduced by removing an explicit requirement for Registered Entities to create and maintain baseline configuration documentation.

Establishing and maintaining baseline configurations represent best practices for system hardening. Texas RE recommends adhering to NIST Special Publication 800-53 (Rev. 5), CM-2 Baseline Configuration, which states, "Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture."

NIST Special Publication 800-53 (Rev. 5) provides additional information, such as using tools to track version numbers on operating systems, applications, types of software installed, and current patch levels in order to maintain the currency, completeness, accuracy, and availability of the baseline configurations of systems. This is information that is currently captured within existing baseline documentation requirements.

If the drafting team has concerns that maintaining baseline documentation of dynamic VMs is not technically feasible, Texas RE suggests adding the verbiage “per system capability” to CIP-010 R1’s baseline requirements. Registered Entities have demonstrated that the vast majority of systems, both physical and virtual, are capable of having baseline documentation created, tracked, and updated as necessary. As such, this requirement should remain in place for those systems where it is technically feasible to perform this industry best security practice.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC

Answer	
Document Name	

Comment

Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying CIP-010 to allow for more flexibility in tracking changes to applicable systems while maintaining and even increasing security.

Likes 0	
Dislikes 0	

Response

7. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes or scoping clarifications related to SCI. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

As mentioned earlier, disagree with adding R1.6 to CIP-005 as CIP-005 is written for protections of logical devices and data. This should be restored back to CIP-006 R1 Part 1.10.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST disagrees with proposed changes to CIP-003 and CIP-011 due to the fact proposed changes go beyond conforming changes.

NST disagrees with proposed changes to CIP-009, as omitting SCI from all Requirements and Parts except for R1 Part 1.5 it would establish “implied requirements,” as discussed in our comments on Question 9, below. NST acknowledges that in some recovery situations, it might only be necessary to recover a virtual BES Cyber System and not its supporting SCI. However, given that failure or destruction of an SCI could, in some scenarios, wipe out an entire Control Center, NST believes that inclusion of SCI in a Responsible Entity’s recovery plan(s) should be mandatory rather than a suggested best practice.

NST agrees with proposed conforming changes to CIP-004, CIP-006, CIP-008 and CIP-013.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section’s scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident

For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says “Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;” Request clarification on execution of what? Perhaps “execution” should be changed to “entity use”

For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC

For CIP-006, Part 1.3 consider changing from “per system capability” because “per system capability” is an inadvertent get-out-of-jail.

For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2

For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with “all” in the new language. The new Part 1.2.5 says “ Verification of software integrity and authenticity of all software and patches provided by the vendor . . .” The R1 applicable systems language is “for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI).” We suggest that the scope should be “applicable systems,” not all software and patches by the vendor.

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident

For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;" Request clarification on execution of what? Perhaps "execution" should be changed to "entity use"

For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC

For CIP-006, Part 1.3 consider changing from "per system capability" because "per system capability" is an inadvertent get-out-of-jail.

For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2

For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with "all" in the new language. The new Part 1.2.5 says " Verification of software integrity and authenticity of all software and patches provided by the vendor . . ." The R1 applicable systems language is "for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI)." We suggest that the scope should be "applicable systems," not all software and patches by the vendor.

Likes 0	
Dislikes 0	

Response

Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC

Answer	No
Document Name	

Comment

For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident

For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;" Request clarification on execution of what? Perhaps "execution" should be changed to "entity use"

For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC

For CIP-006, Part 1.3 consider changing from "per system capability" because "per system capability" is an inadvertent get-out-of-jail.

For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2

For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with “all” in the new language. The new Part 1.2.5 says “ Verification of software integrity and authenticity of all software and patches provided by the vendor . . .” The R1 applicable systems language is “for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI).” We suggest that the scope should be “applicable systems,” not all software and patches by the vendor.

Likes 0	
Dislikes 0	

Response

Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo

Answer	No
Document Name	

Comment

Same comment as for CIP-010, Q6.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section’s scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident

For CIP-003, Attachment 1, 5.1, requests clarification of the new bullet which says “Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;” Request clarification on the execution of what? Perhaps “execution” should be changed to “entity use”

For CIP-004, R5 requests confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC

For CIP-006, Part 1.3 consider changing from “per system capability” because “per system capability” is an inadvertent get-out-of-jail.

For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2

For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with “all” in the new language. The new Part 1.2.5 says “ Verification of software integrity and authenticity of all software and patches provided by the vendor . . .” The R1 applicable systems language is “for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI).” We suggest that the scope should be “applicable systems,” not all software and patches by the vendor.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

For CIP-003, Attachment 1, Section 4, request confirmation that, while this Section has no updates, this Section’s scope is being expanded because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident .

For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says “Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;” The language should be clarified to explain the word “execution” (i.e., on execution of what?) Perhaps “execution” should be changed to “entity use”.

For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents due to the updated definitions of IRA and ERC.

For CIP-006, Part 1.3 consider changing from “per system capability” because “per system capability” is an inadvertent “get-out-of-jail free card.

For CIP-011, the double jeopardy between R2 and Part 1.2 should be clarified.

For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. The use of the word “all” in the new language is of concern. The new Part 1.2.5 says “ Verification of software integrity and authenticity of all software and patches provided by the vendor . . .” The R1 applicable systems language is “for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI).” The scope should be “applicable systems,” not all software and patches by the vendor.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

No: Application Containers need to be defined with additional clarity.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)

Answer	No
Document Name	

Comment

For CIP-006, Part 1.3, consider changing from "per system capability" to "if technically feasible" because "per system capability" is an inadvertent get-out-of-jail.

For CIP-011, the SRC requests clarification on the double jeopardy between R2 and Part 1.2. Both sections apply to the handling and use of BCSI. If you violate R2, you will have mishandled or misused R1.2.

*For CIP-013, Part 1.2.5, consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with "all" in the new language. The new Part 1.2.5 says " Verification of software integrity and authenticity of all software and patches provided by the vendor . . ." The R1 applicable systems language is "for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI)." We suggest that the scope should be "applicable systems," not **"all"** software and patches by the vendor.*

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern agrees with the conforming changes or scoping clarifications related to SCI made to the various CIP standards.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed conforming changes to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying the rest of the CIP Standards to allow for implementing future technologies while maintaining and even increasing security.

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E supports the conforming changes to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
For the proposed CIP-008, the Applicability would include, “An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or Shared Cyber Infrastructure supporting a BES Cyber System.” Note that by a literal reading of this, an SCI supporting EACMS would not be in scope for CIP-008 whereas a traditional EACMS would be.	
Likes 0	
Dislikes 0	
Response	

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
For the proposed CIP-008, the Applicability would include, “An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or Shared Cyber Infrastructure supporting a BES Cyber System.” Note that by a literal reading of this, an SCI supporting EACMS would not be in scope for CIP-008 whereas a traditional EACMS would be.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments that were submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	

Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the conforming changes and scoping clarifications made to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes

Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
(1) The proposed language in in CIP-006-7, R1, Part 1.3, points to system capability, but there are concerns with situations where the PACS is capable, but there is a limitation with a particular physical access device. It seems as thought that may present a gap in the proposed language. As an example, an entity currently has a TFE for a limited physical access device where two factor cannot be applied, such as a roof hatch where it is not possible to install a locking mechanism controlled by the PACS system. Under the approved TFE, additional measures are taken to secure that physical access point. The concern with the proposed language is that the roof hatch may be seen as a physical access device rather than a system. In this instance, the PACS is capable of two-factor authentication, but two-factor authentication cannot be applied to that particular physical access device. Because of this potential and unintended gap, we recommend using the language “per system or device capability.” **(2) For CIP 009-7, Requirement R1, Part 1.1, please consider adding the language SCI supporting an Applicable System” in the Applicable Systems column**.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF	
Likes 0	
Dislikes 0	

Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Israel Perez - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

JT Kuehne - AEP - 6

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Benjamin Winslett - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Melanie Wong - Seminole Electric Cooperative, Inc. - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	

Likes 0

Dislikes 0

Response

patricia ireland - DTE Energy - 4, Group Name DTE Energy

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

James Baldwin - Lower Colorado River Authority - 1

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	

8. The SDT has revised the Implementation Plan to include 3 defined early adoption dates as options should Responsible Entities choose to do so. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

PNMR believes early adoption of the revised CIP standards and definitions is beneficial but proposes that Responsible Entities are not tied to only three early adoption choices (6, 12, or 18 months) after approval of the new standards. PNMR proposes that Responsible Entities still follow notifying their Regional Entities of their early adoption choice within fifteen calendar days of making that decision, but that Responsible Entities have the ability to early adopt at any time between 6 months and 24 months. If, for example, a Responsible Entity is not able to early adopt at the 6-month mark but would be able to 8 months after the approval of the new standards, the Responsible Entity should be able to early adopt and not have to wait an additional 4 months until the 12-month mark.

An alternate proposal would be for the Responsible Entity to notify the Regional Entity of its 6, 12, or 18-month early adoption date but have the ability to change its early adoption date if it is realized before the agreed-upon early adoption date that the Responsible Entity would not be able to be compliant with the new standards by that date. In this case, the Responsible Entity could move its early adoption from 6 months to 12 months, for example.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

With the implementation of compliance oversight plans (COP)s, many entities, particularlylarger entities, are experiencing more frequent audits. 36 months may be more appropriate for an implmentation period based on the scope of the changes being proposed under this project.

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes

Document Name	
Comment	

Cleco agrees with EEI comments.

Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	
Comment	

EEI supports the revised Implementation Plan as proposed.

Likes 0	
Dislikes 0	
Response	

Kimberly Turco - Constellation - 6

Answer	Yes
Document Name	
Comment	

Kimberly Turco, on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	
Response	

Alison Mackellar - Constellation - 5

Answer	Yes
Document Name	
Comment	

Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
RF agrees with the inclusion of the 3 defined early adoption dates as options should Responsible Entities choose to do so with the understanding that all Standards and Requirements will be adopted at that same time.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the revised Implementation Plan and the three (3) defined early adoption dates.	
Likes 0	
Dislikes 0	
Response	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Xcel Energy supports EEI comments and thanks the SDT for working on creating an implementation plan that will allow for enough time for a successful implementation while also allowing for early implementation for entities looking to employ virtualized technologies at a faster pace.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed Implementation Plan.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern understands and agrees with the revised implementation plan which includes 3 defined early adoption dates as an option. Southern also understands that if one of the options were chosen, we would have 15 calendar days to notify our Regional Entity of the selected option.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Diana Torres - Imperial Irrigation District - 6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer	
Document Name	

Comment

“See comments submitted by the Edison Electric Institute”

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE continues to be concerned there is conflicting language in the planned changes section of the implementation plan, as well as language in the unplanned changes section in the proposed implementation plan that could result in a reliability gap.

Regarding the conflicting language addressing planned changes, Texas RE notes that the second paragraph in the proposed implementation plan states: “For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.”

Texas RE understands this language to mean the BCS at the substation must be compliant upon the commissioning of the substation. Texas RE agrees with this position.

However, the first and third paragraphs in the proposed implementation plan appears to conflict with this reading. Specifically, the first paragraph states: “Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.” Furthermore, the proposed implementation plan’s third paragraph states: “For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable

requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan." Texas RE understands this language to mean the BCS at the substation is not required to be compliant until the Registered Entity has performed its annual assessment under CIP-002 R2. This introduces a reliability gap as assets that were commissioned shortly after the entity has completed a CIP-002 R2 evaluation will not be required to be evaluated for up to 15 calendar months, and therefore would not be required to be compliant with the applicable cyber security requirements. Texas RE does not agree with this position. Additionally, there are no requirements to identify PACS, EACMS, or PCAs. Regarding the proposed implementation plan's concerning unplanned changes, Texas RE is concerned the language could be read to result in a reliability gap. Specifically, the first paragraph of the implementation plan states "Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2." Texas RE notes that while it is true that during a CIP-002 R2 review an entity may discover that a BCS now meets a higher BCS threshold than it previously held, this is not the only situation in which an entity may become aware of the need for a higher categorization. For example, if an entity is informed by their RC, PC, or TP that an asset is critical to the derivation of an IROL then the knowledge that the systems must meet the medium impact criteria is immediate and as such the 12-month timer to implement medium impact controls should begin immediately. As written, the language in the implementation plan could result in a situation where a Registered Entity could delay the implementation of medium impact controls at such a substation or power plant for up to 27 calendar months, if the IROL notification arrived immediately after a CIP-002 R2 evaluation. Texas RE recommends the SDT revise the proposed implementation plan language around "unplanned changes" to preclude this result.	
Likes 0	
Dislikes 0	
Response	

9. Please provide any additional comments for the standard drafting team to consider, if desired.

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer	
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment

Southern suggests that the definition for “Cyber System” be modified to eliminate the “A group of” language and simply begin with “One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.”

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	
Document Name	

Comment

NST disagrees with the SDT decision to not compel Responsible Entities to identify and maintain a list of SCI that support BES Cyber Systems in CIP-002. In order to demonstrate compliance with various CIP-003 – CIP-013 requirements for SCI, a Responsible Entity would surely have to demonstrate that all its SCI were accounted for. NST is aware of the fact there is no existing CIP requirement to maintain an inventory of “associated” devices including PCAs, EACMS, and PACS, but doing so was some years ago memorably characterized by a well-known representative of a Regional Entity as an "implied requirement." NST believes an SDT goal should be to avoid adding to the list of "implied requirements."

NST believes the proposed “Exemption” statement in every CIP Standard, 4.2.3.3, “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an Electronic Security Perimeter (ESP) that extends to one or more geographic locations” is both confusing and inaccurate. One provides for the confidentiality and integrity of data, not ESPs. N&ST suggests rewording that’s consistent with the language of proposed CIP-005 Requirement R1 Part 1.4, such as “Cyber Systems associated with communication links used to span a single ESP among two or more geographic locations.”

NST notes the second of two proposed "Measures" for CIP-007 R1 Part 1.3 suggests evidence of compliance with the "non-sharing" of SCI CPU and memory requirement could include "Hardware partitioning of physical Cyber Assets." If our understanding of "hardware partitioning" is correct (that it means, for example, all the Medium Impact BCS that co-reside with High Impact BCS on a single hardware platform are moved to different hardware), then according to the proposed definition of SCI, the end result of "hardware partitioning" would be one or more hardware platforms that are no longer SCI, which would render all proposed requirements for SCI, including CIP-007 R1 Part 1.3, inoperable.

Likes 0

Dislikes 0

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer

Document Name

Comment

AZPS has no additional comments for the standard drafting team to consider currently.

Likes 0

Dislikes 0

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer

Document Name

Comment

No additional comments.

Likes 0

Dislikes 0

Response

Israel Perez - Salt River Project - 6

Answer

Document Name

Comment

We still have concerns on CIP-010-5 because the draft does not include the Guidelines and Technical Basis section where it defines what must be included in a vulnerability assessment. It is understood that the Standards Drafting team emphasizes backwards compatibility, but, the proposed changes to CIP-007 R1 and CIP-010 R1.1 could affect what is required in the vulnerability assessments. At the very least, we would like to know and comment on what additional items will be required for SCI in a vulnerability assessment as there is nothing found in the current proposed changes.

Lastly, under CIP-010 R3.3 BES Cyber System is shortened to BCS. However, this is different than the other parts of CIP-010 R3. We recommend consistency.

Likes 0

Dislikes 0

Response

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer

Document Name

Comment

Although not directly revised in this draft, two issues in CIP-007 deserve mention. Requirement 3.3 obstructs smooth updates of antimalware signatures with large administrative cost and compliance risk, for very little, if any, reliability benefit, and is actually impossible with many automated systems today. The requirement should be revised to remove the testing of signatures. Additionally, CIP-007 R5 language inherited from earlier versions requiring at least 8 character passwords is outdated. SIGE suggests requiring at least 15 character passwords, where capable.

Likes 0

Dislikes 0

Response

John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho

Answer

Document Name

Comment

No additional comments

Likes 0

Dislikes 0

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	
Document Name	

Comment

None at this time.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment

Although not directly revised in this draft, two issues in CIP-007 deserve mention. Requirement 3.3 obstructs smooth updates of antimalware signatures with large administrative cost and compliance risk, for very little, if any, reliability benefit, and is actually impossible with many automated systems today. The requirement should be revised to remove the testing of signatures. Additionally, CIP-007 R5 language inherited from earlier versions requiring at least 8 character passwords is outdated. CEHE suggests requiring at least 15 character passwords, where capable.

Likes 0	
Dislikes 0	

Response

Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC

Answer	
Document Name	

Comment

Xcel Energy supports EEI comments and would like to acknowledge the SDT for their hard work over the years in developing a very difficult and technological set of standards that allow for both backward compatibility and inclusion of future technologies.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	

Response

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	
Document Name	

Comment

PG&E wishes to thank the SDT for their several years of effort in getting these modifications close to completion.

Likes 0	
Dislikes 0	

Response

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	
Document Name	

Comment

The proposed revised definition for EACMS would add the phrase, “Shared Cyber Infrastructure (SCI)” to the definition. The term “SCI” can refer to a system that is supporting PACS or EACMS. If the definition is read in terms of this type of SCI as it pertains to the EACMS definition, that opens the possibility that the scope of an EACMS could be read as applicable to Cyber Assets that perform electronic access control or monitoring of SCI “EACMS/PACS,” thus potentially creating a hall of mirrors effect. The MRO NSRF are not certain how probable or not such an interpretation may be, but prefer that this be addressed here rather than when it’s too late to do so. The MRO NSRF ask that the SDT consider this issue and make any edits necessary to address.

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	

Response

Scott Kinney - Avista - Avista Corporation - 3

Answer

Document Name

Comment

See comments provided by Mike Magruder and/or Glenn Farmer

Likes 0

Dislikes 0

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC

Answer

Document Name

Comment

The use of the terms routable protocol communications, bi-directional routable protocol connection and IP Protocol communications, throughout the standards and the definitions is inconsistent and should be evaluated to determine the necessity of using this different language. If providing the consistency through the standards is not an option, it would be better to put these into the definitions so that entities can differentiate one from the other.

The language in CIP-010 R1.1 appears to be getting further away from acceptable language with each iteration of the requirement. Moving requirements to the Measures column does not make the changes any more security objective focused.

Same comments for CIP-005 R1.2 in that the requirements to document a reason for routable protocol communications should be in the Requirements and not the Measures. Examples of the justification/reason are fine in the Measures, but the requirements should be in the Requirements column.

Likes 0

Dislikes 0

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer

Document Name

Comment

WEC Energy Group is in agreement with the MRO NSRFs comment - "We also wish to raise attention to the proposed change of using the phrase “per system capability,” in place of the previous phrasing “where technically feasible.” While we do not wish for TFE to remain part of the compliance paradigm any longer than necessary, we seek assurance that the phrase “per system capability” will indeed be used as an avenue for Registered Entities to demonstrate compliance instead of an opportunity for auditors to find fault with acceptable security and reliability practices."

Likes 0	
Dislikes 0	

Response

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	
Document Name	

Comment

Chelan asks the SDT to consider the real risks and the goals of the CIP standards. CIP has always been about the protection of BES Cyber Assets/Systems and reducing the risk of a compromise or failure of a BES Cyber System which would adversely impact the BES. By definition, BES Cyber Systems are systems that will have direct impact on the BES, so it makes sense to protect those devices most stringently. Protected Cyber Assets also represent a significant risk since there is no network separation between PCAs and their associated BES Cyber System. A VM escape attack executed against a BES Cyber System would be a single exploit to potentially adversely impact the BES.

However, EACMS and PACS devices do not have a direct impact on the reliability of the BES, and are segregated from BES Cyber Systems and Protected Cyber Assets by protections required by CIP-005. A successful VM escape against a EACMS or PACS device would require a second attack for there to be an adverse impact to the BES.

The new affinity requirements increase both the risk of an adverse impact, by reducing the availability of the in-scope VMs and increase the risk of non-compliance, by forcing the use of a control not meant for this purpose. The requirements proposed essentially create six groups of devices that potentially may not share CPU or memory:

1) High Impact BCS/PCA (including EACMS and PACS classified as PCAs, excluding Intermediate Systems)

2) High Impact EACMS/PACS (outside the ESP)

3) Medium Impact BCS/PCA (including EACMS and PACS classified as PCAs, excluding Intermediate Systems)

4) Medium Impact EACMS/PACS (outside the ESP)

5) Potentially Low Impact BCS

6) Out-of-Scope Devices

This means that a RE would have to establish up to 6 separate resource pools to comply with the definition of PCA and the text of CIP-007 R1.3. Assuming you can group devices in the affinity rule sets you create (this may not be possible on all platforms), this would require 15 separate anti-affinity rules, in addition any existing rules required for resource management purposes.

With the updated language suggested in Question 4, there would only be 3 resource pools needed:

1) High Impact BCS/PCAs (including EACMS and PACS classified as PCAs, excluding Intermediate Systems

2) Medium Impact BCS/PCA (including EACMS and PACS classified as PCAs, excluding Intermediate Systems)

3) All other devices.

Only 3 anti-affinity rules are needed here to satisfy the suggested requirements. This greatly reduces the complexity of the DRS rules needed to satisfy the security objective to protect the BES from the threat of VM escape attacks and decreases the risk of that a BES Cyber System is unable to find a host to run in the event of a failure of one or more SCI hosts.

Likes 0

Dislikes 0

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer

Document Name

Comment

MPC supports comments that were submitted by the MRO NERC Standards Review Forum.

Likes 0

Dislikes 0

Response

Kristine Martz - Amazon Web Services - 7

Answer

Document Name

Comment

The SDT is clear that this project SAR focuses on on-premise virtualization, however, many virtualization concepts convey use of cloud. AWS suggests explicitly stating whether these new terms/requirements, specifically SCI, will apply to cloud or not. If these terms/requirements do not apply to cloud, it should be obvious to the reader.

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer

Document Name

Comment

Conflating support for both High-, Medium-, and Low-Impact Cyber Assets within a single Virtualization Cluster will create additional questions and interpretations between Responsible Entities and ERO Enterprise staff. Clusters by their very nature include pools of shared SCI to include CPU, Memory, Disk, and network resources that are shared between all Cluster members to allow for balancing resources, recovery from failed hardware, and maintaining high availability. The complexity required to balance these pooled resources using affinity rules or logical boundaries to disallow different impact levels of VM guests from running on the same physical resources could be high. Moving VM guests can take place without the need for clustering and would allow for segregated siloing of different impact Cyber Assets without the requirement of determining high-water marking every time a VM guest is moved. Communications play a key role in determining the current health and configuration of clusters – especially with heartbeats and SCSI data requests. Responsible Entities have a high bar to assure that these communications are not to the point that they create common networking connections that would start to include additional VM Guests as PCA.

Marrying both ESP and zero-trust within an overall ESP would better serve our Responsible Entities and create a more secure environment as zero-trust Cyber Assets would not be internet-facing while simplifying the management of the environment. Maintaining the ESP, and fully incorporating virtualization and zero trust paradigms within an identified ESP allows Responsible Entities to leverage another layer of defense (defense-in-depth) for BCS by limiting ingress/egress points and access to these Cyber Assets.

Likes 0

Dislikes 0

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer

Document Name

Comment

"Responsible Entity" is used multiple times in the CIP standards and is not a defined term or a proposed defined term. The standard drafting team may consider defining this term in the NERC Glossary of Defined Terms.

AECI supports the efforts and commitment of the standards drafting team to indutry when soliciting feedback and proposing solutions to identified gaps in the draft standards.

Likes 0

Dislikes 0

Response

Alison Mackellar - Constellation - 5

Answer

Document Name

Comment

Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends clear and concise language on the categorization and impact rating the hosting virtualization infrastructure should have. Specifically, Texas RE recommends eliminating the Shared Cyber Infrastructure definition. Virtualization infrastructure should inherit the highest impact rating and categorizations of the VCAs that the virtualization infrastructure is hosting. For example, if virtualization infrastructure is hosting two	

high impact BCS, three PCAs associated with high impact BCS, and an EACMS associated with high impact BCS, then the virtualization infrastructure should be categorized as a high impact BCS. Implementing high watermarking practices would ensure that the virtualization infrastructure is more reliable and secure.

Texas RE continues to note that no matter how many controls are applied there will always be a parent and child relationship between host and VM's. If the hypervisor is compromised, then all VM's can be. Additionally, if a VM is compromised the same can be true, other VM's and the Hypervisor can be impacted. The Hypervisor should be high watermarked to whatever VMs are on it. Any VMs on the hypervisor should also be marked at the highest impact rating. Different applicable systems with varying impact level lends itself to mixed-trust concepts. This change potential opens the door to allow more corporate based systems (payroll, custom software, etc.) to be on the same hypervisor as CIP applicable systems. CPU and memory segregation only may not protect from vulnerabilities such as hyperjacking, VM escape, Denial of Service, etc.

Likes 0

Dislikes 0

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer

Document Name

Comment

No additional comments.

Likes 0

Dislikes 0

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer

Document Name

Comment

"See comments submitted by the Edison Electric Institute"

Likes 0

Dislikes 0

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

See comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6

Answer	
Document Name	

Comment

We would like to thank the Project 2016-02 SDT on their hard work, dedication, and continuing to listen to industry feedback to meet the FERC order and not create significantly more compliance burden.

Likes 0	
Dislikes 0	

Response

Diana Torres - Imperial Irrigation District - 6

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	

Document Name

Comment

It is unclear in the draft CIP-002-7 how the classification hierarchy is impacted. What is the hierarchy of the SCI classification? Is dual classification with SCI expected??

Likes 0

Dislikes 0

Response

Wesley Maurer - Wesley Maurer On Behalf of: Teresa Krabe, Lower Colorado River Authority, 5, 1; - Wesley Maurer

Answer

Document Name

Comment

LCRA would like to seek clarification regarding virtualization of EACMS outside of an ESP. If the host has in-scope EACMS as well as out of scope virtualized machines, would the same rules apply as SCI within a the ESP? There would be SCI associated with an EACMS. There would be an EACMS that is a virtual machine. Are affinity rules the only compliance obligation associated with the out of scope VM?

Likes 0

Dislikes 0

Response

James Baldwin - Lower Colorado River Authority - 1

Answer

Document Name

Comment

LCRA would like to seek clarification regarding virtualization of EACMS outside of an ESP. If the host has in-scope EACMS as well as out of scope virtualized machines, would the same rules apply as SCI within a the ESP? There would be SCI associated with an EACMS. There would be an EACMS that is a virtual machine. Are affinity rules the only compliance obligation associated with the out of scope VM?

Likes 0

Dislikes 0

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)

Answer	
Document Name	

Comment

In future postings, for definitions, it would be helpful if the table for the definitions could include each standard where the definition appears.

In closing, SRC reiterates that our gravest concern is with proposed changes to CIP-010, Part 1.1 and Part 2.1 which do away with the concept of "baseline changes." The proposed language of "settings changes" goes beyond what was previously in the CIP standards such that we believe they are no longer backwards compatible. SRC proposes "settings changes" be modified to "configuration changes" or eliminated altogether.

Additionally, the SRC would like for the SDT to consider that the standards process has taken very long and there are newer technologies that are not being addressed with these changes.

Likes 0	
Dislikes 0	

Response

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	
Document Name	

Comment

Alliant Energy supports the comments submitted by the MRO NSRF

Likes 0	
Dislikes 0	

Response

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2016-02 Modifications to CIP Standards | Virtualization - Draft 4
Comment Period Start Date:	8/17/2022
Comment Period End Date:	10/7/2022
Associated Ballot(s):	2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 AB 4 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 AB 4 ST

There were 72 sets of responses, including comments from approximately 188 different people from approximately 121 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Director, Standards Development Latrice Harkness (via email) or at (404) 858-8088..

Questions

1. The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

2. The SDT modified other definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

3. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

4. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

5. The SDT has used phrasing such as “SCI supporting an Applicable System from this Part” in the Applicable Systems column across many of the standards. Is it clear that this scopes the requirements for SCI to match the system(s) it hosts?

6. The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

7. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes or scoping clarifications related to SCI. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

8. The SDT has revised the Implementation Plan to include 3 defined early adoption dates as options should Responsible Entities choose to do so. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

9. Please provide any additional comments for the standard drafting team to consider, if desired.

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
WEC Energy Group, Inc.	Christine Kane	3		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					Marc Donaldson	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
MRO	Kendra Buesgens	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Christopher Bills	City of Independence Power & Light	3,5	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Jamie Monette	Allete - Minnesota Power, Inc.	1	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern Power Administration	1	MRO
					Matthew Harward	Southwest Power Pool, Inc.	2	MRO
					LaTroy Brumfield	American Transmission Company, LLC	1	MRO
					Bryan Sherrow	Kansas City Board Of Public Utilities	1	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO
					Jamison Cawley	Nebraska Public Power	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					David Heins	Omaha Public Power District	1,3,5,6	MRO
					George Brown	Acciona Energy North America	5	MRO
					Jaimin Patel	Saskatchewan Power Corporation	1	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Tricia Bynum	FirstEnergy - FirstEnergy Corporation	6	RF
					Mark Garza	FirstEnergy-FirstEnergy	4	RF
Public Utility District No. 1	Meaghan Connell	5		PUD No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1	3	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
of Chelan County						of Chelan County		
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Glen Pruitt	Public Utility District No. 1 of Chelan County	6	WECC
					Meaghan Connell	Public Utility District No. 1 Chelan County	5	WECC
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					James Mearns	Pacific Gas and Electric Company	5	WECC
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Dana Showalter	Electric Reliability	2	Texas RE

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
				(SRC) 2016-02 Virtualization (Draft 4)		Council of Texas, Inc.		
					Helen Lainis	IESO	2	NPCC
					Kathleen Goodman	IS-NE	2	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Michael Del Viscio	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SERC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Jim Howell	Southern Company - Southern	5	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Company Services, Inc. - Gen		
DTE Energy	patricia ireland	4		DTE Energy	Patricia Ireland	DTE Energy - Detroit Edison	4	RF
					Karie Barczak	DTE Energy - Detroit Edison Company	3	RF
					Adrian Raducea	DTE Energy - Detroit Edison Company	5	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC Regional Standards Committee	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Harish Vijay Kumar	IESO	2	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					David Kiguel	Independent	7	NPCC
					Nick Kowalczyk	Orange and Rockland	1	NPCC
					Joel Charlebois	AESI - Acumen Engineered Solutions International Inc.	5	NPCC
					Mike Cooke	Ontario Power Generation, Inc.	4	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Shivaz Chopra	New York Power Authority	5	NPCC
					Deidre Altobell	Con Ed - Consolidated Edison	4	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Cristhian Godoy	Con Ed - Consolidated Edison Co. of New York	6	NPCC
					Nurul Abser	NB Power Corporation	1	NPCC
					Randy MacDonald	NB Power Corporation	2	NPCC
					Michael Ridolfino	Central Hudson Gas and Electric	1	NPCC
					Vijay Puran	NYSPS	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					Sean Cavote	PSEG - Public Service Electric and Gas Co.	1	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					John Pearson	ISONE	2	NPCC
					Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
					Chantal Mazza	Hydro-Quebec	2	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD / BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					William Price	M and A Electric Power Cooperative	1	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Cooperative, Inc.		
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The SDT has modified the IRA definition to simplify it, primarily in regards to the routable protocol to serial conversion scenario. Do you agree with the proposed change? If not, please provide the basis for your disagreement and an alternate proposal.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST sees no reason to change the existing definition's use of "remote access client or other remote access technology." The second part of the proposed definition would, as written, apply to any remote connection using a communications path that included routable to serial conversion, regardless of where that conversion took place (e.g., remote location vs. "local," or "inside the BES asset" location). NST is aware of concerns that using phrases such as "outside the asset" in this context might cause confusion about its relationship to electronic access control requirements for BES assets containing low impact BCS, but we nonetheless recommend using it to avoid overly broad application of "IRA" to communications using both routable and serial wide-area connections.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT asserts that the scenario must meet the definition of IRA in order to be in scope of the requirement. The current definition is not clear as to whether a device that is serial only, and thus has no "associated ESP", can have IRA at all. The SDT is making this scenario clear in scope of the definition, so that the requirements in CIP-005 R2 are applied. The SDT also removed phrases such as "outside the asset" and "remote access client or other remote access technology." in response to previous comments concerning what those terms mean, especially now with the use of SSL VPNs and other methods that require no client "remote access" software.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

The term “Cyber System” is too broad in scoping IRA. Suggest revise to clarify that the target of IRA is BES Cyber System rather than “Cyber System” to avoid including EACMS, SCI, PCA, etc.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Definitions and scoping are separate, therefore, do not scope requirements. The SDT, by defining the glossary term IRA, is describing a type of access. Similarly, in defining Cyber System, the SDT is describing a collection of Applicable System types that are collectively referred to as the defined term. The Glossary of Terms is the dictionary for what each term means. The scoping of CIP requirements is achieved through requirement language where the term is used, in combination with the Applicable Systems column for each corresponding Requirement Part.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC

Answer	No
Document Name	

Comment

Under the new definition of IRA, bullet 5 that excludes “Communication that originates from an Intermediate System; or,” should not be excluded from the definition. Excluding it would be confusing as IRA to a BCS should come from an Intermediate System.

The new definition of IRA conflicts with the existing definition of ERC. ERC is the ability to access a BCS through its ESP via a “bi-directional” routable protocol connection.

In the new IRA definition, the second bullet addressing serial Cyber Assets states that IRA is “User-initiated electronic access by a person using a routable protocol” (*not necessarily bi-directional*), “that is converted by the Responsible Entity to a non-routable protocol….,” is in direct conflict with the existing definition of ERC. This is not a concern over serial end points being in scope or not, we all agree that they are in scope, but the term “bi-directional” does nothing to help bring serial devices into scope, in fact it implies that serial devices that do not establish TCP/IP connections are out of scope.

Our recommendation to the SDT is to modify the definition of ERC as follows. First, remove the words “bi-directional” since there is no such thing as bi-directional routable protocol. Changing the ERC definition to simply “routable protocol” would create consistency throughout the

requirements. Second, remove the word “connection” as this term implies that there has been a TCP handshake and a connection is established while excluding connectionless protocols such as UDP. Consider using “routable protocol communication” or just “routable protocol”. In CIP-005 R1.2, reference is made to routable protocol communication instead of connection, so the SDT may want to align with that if they are using the term routable protocol is not enough.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees “Communication that originates from an Intermediate System; or,” should not be excluded from the IRA definition and has removed that phrasing. The SDT decided to retain the proposed language in the ERC definition. The SDT asserts IRA describes a particular access type, whereas ERC describes a transport mechanism for which the access type of IRA is accomplished. The ERC definition is used as a scoping mechanism within the Applicable Systems of Requirement Parts, whereas IRA itself is an access type for which particular controls defined in CIP-005 R2 must be implemented. The SDT addressed the concern about directionality of the routable protocol connection within the IRA definition by clarifying IRA, including "...using a routable protocol • That is converted by the Responsible Entity to non-routable protocol "that allows access" to a Cyber System;...".	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	No
Document Name	
Comment	
Should “or” be added to the end of the first bullet to more clearly define the need to continue dropping through the bullets like a decision tree to identify if any of the points are true instead of exiting after the first question? It is unclear if after the first bullet is an “and” or an “or” to identify IRA.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Reference the word version of the Results-based Standard template (link) on the NERC Resource page. Numbered lists indicate an “and” and bulleted lists indicate an “or.” The location of the “or” means that each bullet would read with an “or” as you move to the next bullet.	

Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Changes to the IRA definition adds conversion from routable to non-routable (serial) communications to remote BCS that was previously omitted. Further clarifications in the definition of IRA removes some gray areas and further delineates IRA from system-to-system communications. However, there remains a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication but have not enforced protections to ensure that malicious actors do not use the ports – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to the definition to ensure validity of communications to Applicable Systems regardless of source or intent. In addition, approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization and approval of SCI terminology and other definitions associated with virtualization. The SDT has added rationale but not defined whether user-created scripts and programs that can be modified and scheduled to run independently are considered IRA – even though an unauthorized user could modify it to their benefit. Both scripts and programs can be user-initiated, and with no definition of system-to-system communications there are still lingering issues regarding what system-to-system communications is comprised. Further, user-created scripts and programs may not be capable of reading multi-factor tokens or their displayed codes, but additional security for these connections can be implemented through certificates and the use of secure connections via SSH or SSL.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT maintains there is a long standing issue where "system to system" communications (covered by CIP-005 R1) could need and use protocols/ports that can also be used for IRA. The SDT asserts that IRA is focused on the human interaction with the Applicable System and the associated capability for a human to access and remotely interact with an Appliable System. Not the interactive capability of a given protocol/port that may also be needed for process-based system-to-system communication, relying on other CIP-005 and CIP-007 requirements to restrict communications and secure the Applicable System. If a protocol is used for IRA, then CIP-005 R2 controls must be applied to that access. However, the R2 controls are designed for interactive users only; Applying those controls to non-user interactive sessions (system-to-system) would break automated system-to-system data transfers and the like that may be needed for reliable operation of the BCS. Therefore, the SDT cannot apply R2 controls in a mandatory manner to these protocols/ports that have multiple uses, such as secure batch file transfers between processes and interactive user logon. The SDT is concerned with how a mandatory requirement preventing IRA (or considering system-to-system communication using certain IRA capable protocols/ports) in these specific situations could be constructed, as in some cases entities may use the protocol/port to	

perform both, while also having the proper controls on both. The SDT has not defined scripts and programs scheduled to run independently as IRA for the reasons noted - the R2 controls would break such functionality.	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
The revised definition of IRA provides more clarity than the earlier version. With that said, AEP recommends removing second bullet under what “IRA does not include” list, as IRA should include “communication that originates from an Intermediate System”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees and made the corresponding change in the definition as well as in requirements to avoid the "hall of mirrors" effect regarding recursive Intermediate Systems, which the bullet was originally intended to prevent.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Request confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. It is up to each Registered Entity to determine which serial connections meet the updated IRA definition and proposed requirement language, and an entity would need to know what Applicable Systems a user can initiate remote access (IRA) to even if the device is serial only. For example, a serial cable from a terminal server connected to the console port of an Applicable System that can be accessed remotely benefits	

from re-evaluation to see if it meets the new definition of IRA and would need CIP-005 R2 controls on the routable protocol part of the overall path. Thus, this is not an evaluation of all serial, but an evaluation where a user can remotely access on the serial side of IP-serial converters/terminal servers only.	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	No
Document Name	
Comment	
Suggest change to ¨To a Management Interface of Shared Cyber Infrastructure protected by an ESP¨. As management interface of target SCI should be located inside ESP and SCI outside ESP should not be in scope. Request confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. It is up to each Registered Entity to determine which serial connections meet the updated IRA definition and proposed requirement language, and an entity would need to know what Applicable Systems a user can initiate remote access (IRA) to even if the device is serial only. For example, a serial cable from a terminal server connected to the console port of an Applicable System that can be accessed remotely benefits from re-evaluation to see if it meets the new definition of IRA and would need CIP-005 R2 controls on the routable protocol part of the overall path. Thus, this is not an evaluation of all serial, but an evaluation where a user can remotely access on the serial side of IP-serial converters/terminal servers only.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Request confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. It is up to each Registered Entity to determine which serial connections meet the updated IRA definition and proposed requirement language, and an entity would need to know what Applicable Systems a user can initiate remote access (IRA) to even if the device is serial only. For example, a serial cable from a terminal server connected to the console port of an Applicable System that can be accessed remotely benefits from re-evaluation to see if it meets the new definition of IRA and would need CIP-005 R2 controls on the routable protocol part of the overall path. Thus, this is not an evaluation of all serial, but an evaluation where a user can remotely access on the serial side of IP-serial converters/terminal servers only.	
Jodirah Green - ACES Power Marketing - 6	
Answer	No
Document Name	
Comment	
The IRA definition contains “To a Manangement Interface of Shared Cyber Infrastructure”. We feel this should read “To a Management Interface”. Adding SCI to the definition restricts the scope to just Management Interfaces on SCI. Management Interface’s definition contains SCI, so it is unnecessary to put SCI into the requirement as well.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees and changed the definition to "To a Management Interface" and moved all scoping to the standard within the Applicable Systems and Requirement Parts. CIP-005 R1.3 was rewritten to incorporate the security objective of protection of the configuration of ESPs and SCI, leaving the method to the entity.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	

We suggest that IRA definition should remain unchanged and have the specific scenarios that these definition changes are attempting to address become part of the standard requirement language. (i.e. CIP-005-8 R2).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT asserts that the scenario must meet the definition of IRA in order to be in scope of the requirement. The current definition is not clear as to whether a device that is serial only, and thus has no "associated ESP", can have IRA at all. The SDT made this scenario clear in scope of the definition, so that the requirements in CIP-005 R2 are applied.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Request confirmation that entities should re-evaluate serial connections because they may now be in scope due to the updated definitions of IRA and ERC.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. It is up to each Registered Entity to determine which serial connections meet the updated IRA definition and proposed requirement language, and an entity would need to know what Applicable Systems a user can initiate remote access (IRA) to, even if the device is serial only. For example, a serial cable from a terminal server connected to the console port of an Applicable System that can be accessed remotely benefits from re-evaluation to see if it meets the new definition of IRA and would need CIP-005 R2 controls on the routable protocol part of the overall path. Thus, this is not an evaluation of all serial, but an evaluation where a user can remotely access on the serial side of IP-serial converters/terminal servers only.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	No
Document Name	

Comment	
The SRC suggests that IRA definition should remain unchanged and have the specific scenarios that these definition changes are attempting to address become part of the standard requirement language. (i.e. CIP-005-8 R2). 1. The SDT modified other definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT asserts that the scenario must meet the definition of IRA in order to be in scope of the requirement. The current definition is not clear as to whether a device that is serial only, and thus has no "associated ESP", can have IRA at all. The SDT made this scenario clear in scope of the definition, so that the requirements in CIP-005 R2 are applied.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the proposed changes for the IRA definition.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	

AZPS agrees with the IRA definition modifications.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
WECC suggests that the CIP-005-8 R2.4 use of ‘vendor remote access’ in the applicable system is not consistent with ‘active vendor remote access sessions’ and causes confusion considering neither term is defined. WECC suggests removing ‘vendor remote access’ from the applicable systems and have the scope of ‘active vendor remote access sessions’ stand on its own.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees and removed the phrase.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE agrees with the revisions to the IRA definition. Use of an Intermediate System to access systems that convert routeable to non-routable protocol adds a mandatory MFA step that may not be present in current implementations, and logs use of those systems.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) agrees with the revisions to the IRA definition. Use of an Intermediate System to access systems that convert routeable to non-routable protocol adds a mandatory MFA step that may not be present in current implementations, and logs use of those systems.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for the hard work in developing this definition.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the revised Interactive Remote Access (IRA) definition.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Chelan appreciates the SDT's work on IRA and CIP-005 and approves the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	

Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Thank you to the SDT for clarifying what is and what is not applicable.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the revised definition of IRA.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
MRO does not understand the need for the qualifier ‘by the Responsible Entity’ added to the conversion to non-routable. This seems like it would give entities a way out of compliance with the IRA requirements around serial communication by having someone else convert it.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT added the phrase in response to comments on previous drafts. For circuits that go between different entities, such as between a BA and a GO/GOP, the generator may only have a serial connection they connect to their system. They do not know whether the serial is converted to IP at any point along the path to the BA. To make this clear, the entity that does the conversion from IP to serial is the one that will need, if IRA is allowed over the path, to implement CIP-005 R2 controls on the IP side of the conversion. The generator cannot do that in this scenario. The SDT asserts that the entity that performs the conversion needs to be concerned, not the entity that simply has a serial cable to connect to. The TR was be modified to address the concern.	

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh

Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Bradley Collard - Pedernales Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	

Document Name	
Comment	
Suggest change to ¨To a Management Interface of Shared Cyber Infrastructure protected by an ESP¨. As management interface of target SCI should be located inside ESP and SCI outside ESP should not be in scope. Request confirmation that entities should re-evaluate serial connections because they may now be in scope . . . due to the updated definitions of IRA and ERC	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees and changed the definition to "To a Management Interface" and moved all scoping to the standard within the Applicable Systems and Requirement Parts. CIP-005 R1.3 was rewritten to incorporate the security objective of protection of the configuration of ESPs and SCI, leaving the method to the entity.	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	

2. The SDT modified other definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No: Application Containers need to be defined with additional clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of application containers as software of a VCA or CA.	
Bradley Collard - Pedernales Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
PEC would like to see the SDT provide clarity regarding virtual machines on a TCA being treated as software, however a VCA running on an SCI is not software, but a CA.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of a VCA on a TCA as software.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
The phrase "actively remediated in an environement" in the PCA and VCA definitions needs to be clarified; additional information on the meaning of that phrase that was included in the technical rationale could be utilized to clarify the definitions. For CIP-003, Attachment 1, Section 4, request confirmation that, while this Section has no updates, this Section's scope is being expanded because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification and an example of remediation and isolation. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1. It has been updated to include SCI as a conforming change.	
Jodirah Green - ACES Power Marketing - 6	
Answer	No
Document Name	
Comment	
See comments from question 1.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1. It has been updated to includes SCI as a conforming change.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro appreciates the opportunity to review and offers the following comments. PCA definition needs clarification. The second bullet refers to a cyber asset being remediated in an isolated environment. It is unclear what remediation and isolation is required. An use case and example would be helpful to explain the intent here.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the updated CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification and an example of remediation and isolation.	
David Jendras - Ameren - Ameren Services - 3	

Answer	No
Document Name	
Comment	
Ameren believes that in the BCSI definition, Shared Cyber Infrastructure should be put in parentheses so that it's clear that SCI is a part of BCSI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the updated BCSI definition, modified to remove the first reference to SCI. It was determined that the threat is to the BCS, and that would extend to any SCI supporting it without having to expressly include it, as shown in the example.	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	No
Document Name	
Comment	
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section’s scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1. It has been updated to include SCI as a conforming change.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	

For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section’s scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1. It has been updated to include SCI as a conforming change.

JT Kuehne - AEP - 6

Answer	No
Document Name	

Comment

AEP supports all proposed definitions with the exceptions of “Cyber Assets” and
“Interactive Remote Access (IRA)”. Our comments are specified below:

- **Cyber Assets**: The SDT added “*Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets*” to the definition of Cyber Asset. AEP suggests deleting the added sentence since it adds more confusion to the definition and it is included in the VCA definition.
- **Interactive Remove Access (IRA)**: Please see our response under Question #1.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of application containers as software of a VCA or CA.

See the response to your comments on Q1.

Lindsey Mannion - ReliabilityFirst - 10

Answer	No

Document Name	
Comment	
Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes. Further, introducing Shared Cyber Infrastructure (SCI) and Management Interface increases the number of Requirements and Parts that a Responsible Entity needs to track compared to simply identifying the hypervisor and associated hardware and “high-water marking” them with the highest identified impact rating BCA/VCA, EACMS, or PACS, and creating a BCS. Further, the ideology surrounding “remediation VLANS” should be revisited to understand the risks posed by implementing such an environment. The complexity required to balance these pooled resources using affinity rules or logical boundaries to disallow different impact levels of VM guests from running on the same physical resources could be high. RF believes that the rationale put forth by the Standards Drafting Team for a “remediation VLAN” and the use of automation of security controls poses additional risks that can be mitigated through the use of Transient Cyber Assets (TCAs) in CIP-010 to accomplish the same vulnerability assessments and updates (OS patches, AV updates, etc.) without the complexity or risk associated with having to identify and unidentify PCAs as they are taken out and placed into service in the production network.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT disagrees as many will not vote to approve terms (particularly technology terms) and definitions in a vacuum with no context as to how those definitions will be used. Also, at times terms are created to match the requirements, such as IRA. Many may say that the IRA definition is too restrictive. However, it is defined so that it matches scenarios where the CIP-005 R2 requirements can be met without affecting functionality or reliability of systems. The inclusion of "remediation VLAN" language is an attempt to address a current risk, based on the order of operations in the use of these tools. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification of the treatment of "remediation VLANS."	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	No
Document Name	
Comment	

The current definition of “Management Interface” still appears to be a bit unclear. It seems to exclude the management interface of a switch inside the Electronic Security Perimeter. NRG recommend changing the third bullet of the definition from “Configures an Electronic Security Perimeter” to “Configures a network device.” Additionally, the proposed “Protected Cyber Assets” definition could be read to include any Virtual Cyber Asset that shares physical CPU or memory, despite the addition of “resources”. We believe the intent of the drafting team to be sharing virtual CPU or memory. If so, the definition should be clarified to read, “any Virtual Cyber Asset sharing the same CPU or memory allocation.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT modified the third bullet of the definition of a management Interface to provide additional clarity. The SDT intends this to be looked at on a physical level. Host affinity is the concept that has been continually discussed, which creates an affinity set within a cluster based on individual physical devices.	
Kristine Martz - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	
AWS agrees with the following proposed definition changes but asks the SDT to consider including the items suggested below in implementation guidance to support entities in adopting the revised definitions: **Interactive Remote Access (IRA):** AWS asks the SDT to consider including the meaning of system-to-system communications in implementation guidance to support entities with implementing the revised IRA definition. We suggest including elements such as where the system-to-system communication originates – inside or outside of the Electronic Security Perimeter (ESP). **Management Interface:** AWS asks the drafting team to consider clarifying the meaning of “administrative interface.” For example, the SDT could clarify if “administrative interface” is intended to include Graphical User Interfaces (GUIs), Command Line Interfaces (CLIs), Software Development Kits (SDKs), and/or Application Programming Interfaces (APIs). **Virtual Cyber Asset (VCA)**: AWS asks the SDT to consider including the meaning of “dormant file-based images” in implementation guidance to support entities with implementing the revised VCA definition. Additionally, AWS suggests including guidance to ensure that security controls are in	

place for dormant file-based images to mitigate vulnerabilities. For example, guidance that includes verification that required cyber security controls are in place prior to using the file-based image in production.

AWS does not agree with the following proposed definition:

Transient Cyber Asset (TCA): The modification to the Transient Cyber Asset definition that allows virtual machines running on a physical TCA to be treated as software on the device should be reconsidered. As written, an entity may not apply the appropriate security controls to the virtual machines running on physical TCAs. Entities should be monitoring the state of the virtual machines running on their physical hardware for security issues. We propose removing the language “Virtual machines hosted on a physical TCA can be treated as software on that physical TCA” from the TCA definition. By removing this language, entities would be required to apply security controls to the virtual machines hosted on their physical TCAs in alignment with CIP-010 R4.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. See the updated CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification of the treatment of VCAs on physical TCAs.

Martin Sidor - NRG - NRG Energy, Inc. - 6

Answer	No
Document Name	

Comment

The current definition of “Management Interface” still appears to be a bit unclear. It seems to exclude the management interface of a switch inside the Electronic Security Perimeter. NRG recommend changing the third bullet of the definition from “Configures an Electronic Security Perimeter” to “Configures a network device.”

Additionally, the proposed “Protected Cyber Assets” definition could be read to include any Virtual Cyber Asset that shares physical CPU or memory, despite the addition of “resources”. We believe the intent of the drafting team to be sharing virtual CPU or memory. If so, the definition should be clarified to read, “any Virtual Cyber Asset sharing the same CPU or memory allocation.”

Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The SDT modified the third bullet of the definition of a management Interface to provide additional clarity. The SDT intends that this be looked at on a physical level. Host affinity is the concept that has been continually discussed, which creates an affinity set within a cluster based on individual physical devices.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
The definition of Protected Cyber Asset carries with it an implicit requirement with the CPU and memory clause. The implication of the requirement is that a VM that is not a Protected BES Cyber Asset may not share CPU and memory with a BES Cyber System. If out-of-scope VM inadvertently shares CPU and memory with a BES Cyber System, then it suddenly becomes a PCA by definition and has instantly violated the majority of the CIP requirements. This is similar to the issue with Intermediate System that was corrected in this draft. Chelan recommends removing the CPU and memory sharing clause and adopt the suggested language in Q4 for CIP-007 R1.3, a requirement that a BCS/PCA may not share CPU and memory with non-BCS/PCA of the same impact level. That would change an inadvertent resource sharing incident into a single violation of CIP-007 R1.3 rather than violating all the requirements that have PCA as an Applicable System. Please see the response to question 4 for suggested language.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT does not agree that the PCA definition imposes implicit requirements, but rather that there are consequences on the placement of VMs. The interaction of the PCA definition with the CIP Requirements has consequences for any item that meets the PCA definition, and this is intentional.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	

WEC Energy Group has a continued concern with the newly defined term "Management Interface". Based on the rationale, it is understood why the need to define these interfaces exists. However, this definition differs from the virtual concept and extends to application functionality tools which, in our opinion, is outside of the intended scope of the Project. Thus bringing additional devices into scope even for those entities that are not using virtual machines. Proposing the SDT remove the 3rd bullet from the definition.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT modified the third bullet of the definition of a management Interface to provide additional clarity. The third bullet of the Management Interface definition, "• Configures an EAP", includes physical devices that can create Virtual Local Area Networks (VLANs) which applies virtualization techniques to the network infrastructure. Further, the SDT contends that the third bullet is necessary to deal with the additional complexity that Zero-Trust architectures bring to the concept of an ESP and EAP.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name
SMUD / BANC

Answer	No
Document Name	

Comment

While updating the definition of EAP for virtualization and to accommodate zero trust architectures, it would be good to also not refer to a “Cyber Asset interface,” as the EAP could be a zone-based implementation, transparent firewall, a single physical interface, multiple physical interfaces, sub interfaces (virtual SVI) or a port channel/group. The term Cyber Asset “interface” is too restrictive.

We recommend the SDT change the definition to “An electronic access or policy enforcement point on an EACMS that controls routable communication to and from one or more BES Cyber Systems and their associated PCAs.”

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The EAP definition is created with two ways to meet the definition. Either as a Cyber Asset Interface, for backwards compatibility, or as a policy enforcement point to accommodate Zero-Trust.

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	No
Document Name	

Comment

Manitoba Hydro thanks the drafting team for considering all comments and implementing changes to the definitions. Manitoba Hydro is in support of the changes to most definitions and the new definitions. For the updated definition of **Electronic Access Control or Monitoring Systems (EACMS)** it appears that the scope has inadvertently been increased with the “SCI” wording. The definition includes Cyber Assets… that perform electronic access control or electronic access monitoring of… SCI. The definition for SCI includes systems that host EACMS and PACS and systems that provide storage resources to EACMS and PACS. The scope of an EACMS would therefore increase to include systems that provide electronic access control and monitoring for SCI supporting EACMS and PACS, however systems providing electronic access control and monitoring directly for EACMS and PACS are not in scope. The definition is the only place where the scope of EACMS is set.

The following wording is suggested:

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s), BES Cyber Systems or SCI supporting applicable Cyber Assets. This includes Intermediate Systems.

Manitoba Hydro also notes a minor clarification in the new definition of Management Interface. It referest to deploying “SCI”, this should actually refer to the VCA hosted on the SCI:

An administrative interface that:

• Controls the processes of initializing or deploying VCA hosted on SCI or

Controls the process of configuring Shared Cyber Infrastructure; or

• Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or

• Configures an Electronic Security Perimeter.

Additionally the definition for VCA includes the term "virtual machine". This is a technology specific term and excludes some potential instances of VCA such as virtualization used in the CISCO Nexus platform. This can be resolved by removing the following wording: "currently executing on a virtual machine"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT appreciates the clarity brought to the concern around the inclusion of SCI as a target of the controls found in the EACMS definition as it was in Draft 4. The EACMS definition was modified to address this concern.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
In the proposed definition of "Cyber Asset", the definition of "application container" versus VCA is unclear. The term "container" used in this definition needs further clarification. In the proposed definition of "Management Interface", the definition of "administrative interface" is unclear. The term "administrative interface" used in this definition needs further clarification. In the proposed definition of TCA, removal of the qualifier "directly" may inappropriately expand the scope of the requirement to include devices connecting via IRA or Intermediate System.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of application containers as software of a VCA or CA. The SDT contends the bullets following the term "administrative interface" in the Management Interface definition are the clarifying qualities that define the term, without requiring a formal definition for "administrative interface", which could cause more confusion than clarity for industry.	

Additionally, the TCA definition was modified in regards to network connectivity for clarity that applies to the removal of the term "directly".	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
Definition of VCA: NST believes the proposed definition of VCA should more closely resemble the existing definition of "Cyber Asset" or, better still, be eliminated altogether. The existing definition of "Cyber Asset" could be easily "unbound" from "hardware" with this or a similar modification: Change from, "Programmable electronic devices, including the hardware, software, and data in those devices" to, "Hardware-based or virtual programmable electronic devices, including the software and data in those devices." Definition of TCA: NST considers the statement in the proposed definition of TCA, "Virtual machines hosted on a physical TCA are treated as software on that physical TCA" to be oddly inconsistent with the proposed definition of VCA. Furthermore, we disagree with the SDT's opinion that if a physical TCA hosts one or more virtual TCAs, there should be no need to track and manage each individual physical and virtual device. Definition of ESP: NST believes the proposed new part of the current ESP definition, “or a logical boundary defined by one or more EAPs” is redundant and unnecessary. We therefore recommend maintaining the currently approved ESP definition. Definition of ERC: NST believes the use of the word, "through (an ESP)" has the potential to cause confusion over what kind of routable communications qualify as ERC. ERC to or from a Cyber Asset should be clearly defined as "through" an ESP boundary or access point, not "through" an ESP (the online Merriam Webster dictionary defines "through" as "a function word to indicate movement into at one side or point and out at another and especially the opposite side of // 'drove a nail through the board'"). NST believes the existing definition of ERC can and should be retained as-is. Definition of EAP: NST believes the proposed definition of EAP is problematic in two respects. First, we believe it could be interpreted to mean an EAP should control all routable communication between a BCS and any other Cyber Asset regardless of whether that "other" device is within or outside of the same ESP protecting the BCS. Second, we believe the SDT should better define "policy enforcement point," lest Responsible Entities, Regional Entities, and NERC develop their own conflicting definitions.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT looked at combining the CA and VCA concepts in the early stages of this project and determined that there were challenges with that approach. First, if virtual based, then the hardware would not be included. Second, the inability to target controls specifically at the virtual versions of things. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of a VCA on a TCA as software, explanations for ESP, and EAP.	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
Greater clarity is needed regarding Cyber Assets, CIP Systems and Cyber Systems. The differences between these terms should be made more explicit, overlaps should be eliminated, and redundant terms should be eliminated also.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. CIP System has been removed as a proposed definition. Cyber Systems is simply a term as shorthand instead of having to reference all the forms that something can have. Refer to the CIP Definitions and Exemptions Technical Rationale document for further clarification.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. See response to EEI.	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
"Management Interface" – the language of the definition still leaves ambiguity of interfaces on other CAs, for example vCenter. It is understood that the intent of the SDT was to only include interfaces on applicable CAs, which could leave those unprotected by the standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. See the updated CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the Management Interface definition.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the modified definitions used in the CIP standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes

Document Name	
Comment	
- NextEra Energy (NEE) encourages the SDT to enhance the clarification of bi-directional routable communication with IRA and ERC. Entities will need to clarify their implementation of bi-directional for routable communications. - Is requiring authentication to a local network or different VLAN considered a logical break?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The definition of IRA was updated to include “bi-directional” in the latest draft after the SDT determined the concept was no longer included by way of the reliance on the External Routable Connectivity definition and is an integral part of Interactivity.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	

Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the modified definitions that will be used for the CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for the hard work in developing these definitions.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments and support. See response to EEI.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE recommends consistent use of “Shared Cyber Infrastructure (SCI)” throughout the definitions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT made some modifications to the use of the term Shared Cyber Infrastructure in the Draft 5 definitions.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
The only disagreement with the proposed defintions is for the CIP Senior Manager. The updated definition for CIP Senior Manager could cause some confusion because it is broad and appears to apply to all the CIP Standards, even though CIP-012 and CIP-014 do not have CIP Senior Manager requirements or responsibilities. An alternate wording could be “.... continuing adherence to the requirements within the NERC Critical Infrastructure Protection Standards in which the CIP Senior Manager has responsibilities"	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT contends the original creation of the term CIP Senior Manager applied across all CIP Standards at the time, and that the role has responsibility and authority over the implementation of all CIP Standards.	

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
SIGE recommends consistent use of “Shared Cyber Infrastructure (SCI)” throughout the definitions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT made some modifications to the term Shared Cyber Infrastructure in the Draft 5 definitions.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the modifications to the definitions, however, would like additional clarity on the meaning of “application container” which is used within the definitions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of application containers as software of a VCA or CA.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern agrees with the proposed changes of the CIP standards definitions. Suggestions for updates have been listed below.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

“See comments submitted by the Edison Electric Institute”

Likes 0

Dislikes 0

Response

See response to EEI.

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE is concerned the proposed definition of Electronic Access Point (EAP) is ambiguous. Texas RE believes the SDT’s intent was to write a definition that applied to communications between BES Cyber Systems and PCAs and Cyber Assets not protected by the same ESP. The proposed definition as written, however, could be interpreted to mean that EAPs are only applicable when controlling communication between a BCS and its PCAs. The proposed language as written could also be interpreted to mean “An electronic policy enforcement point” or “a Cyber Asset interface on an EACMS that controls routable communication to and from one or more BES Cyber Systems and their associated PCAs.”

It could also be interpreted to mean “An electronic policy enforcement point” or “a Cyber Asset interface on an EACMS that controls routable communication to and from one or more BES Cyber Systems and their associated PCAs.

For clarification, Texas RE recommends the following definition:

An EAP is:

- A Cyber Asset interface on an EACMS; or
- An electronic policy enforcement point

that controls routable communications between Cyber Systems protected by an ESP and:

- one or more Cyber Systems that are not protected by an ESP; or
- one or more Cyber Systems that are protected by a different ESP.

Likes 0

Dislikes 0	
Response	
Thank you for your comments. See the updated EAP definition in Draft 5, which clarifies that it is controlling access to or from one or more BCS or their associated PCA.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	
Document Name	
Comment	
For definition of Transient Cyber Asset (TCA): Reconsider the wording of the sentence ¨ Virtual machines hosted on a physical TCA are treated as software on that physical TCA¨. The language used leaves room for misinterpretation and allows entities to use VM on physical TCA to bypass implementing security controls in the VM. VM image security should be verified prior to execution on TCA. For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section’s scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for clarification on the reasoning behind treatment of application containers as software of a VCA or CA. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been updated to include SCI as a conforming change.	

3. The SDT revised CIP-005 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
Disagree with adding R1.6 to CIP-005 as CIP-005 is written for protections of logical devices and data. This should be restored back to CIP-006 R1 Part 1.10.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT feels that R1.6 consolidates requirements together and removes the possibility for double jeopardy.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.	
Likes 0	
Dislikes 0	
Response	

Thank you for your response. R1.3. The SDT has made this requirement more objective to clearly define what is it is intended to accomplish	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	No
Document Name	
Comment	
New requirement to deny access to the Management Interface from BCS and associated PCAs (R1.3). – This would require significant effort for us if approved. As written, the proposed changes appear to require significant modification to our current network architecture without clearly indicating even how this can be accomplished in a compliant fashion or how that improves upon the existing security posture.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response . The SDT made this requirement more objective to clearly define what is it is intended to accomplish.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern does not agree with the proposed change in Part 1.3. The way EACMS is written, it suggests that it includes all forms of EACMS and is too broad. The term “EACMS that enforce an ESP” is not bound to firewalls and switches with VLANs, in other words EACMS that enforce network segmentation. Domain Controllers for example can help “enforce” an ESP in determining who can and can’t cross the ESP. It is not clear, in that case, what the “Management Interface” of a domain controller EACMS is, nor can routable protocol be restricted to it if its used to authenticate users. The original approved standard lists Electronic Access Points for High and Medium BCS which more aligns with equipment within an ESP. Southern suggests considering the use of EAP as the object of this requirement to clarify the scope.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The SDT made this requirement more objective to clearly define what is it is intended to accomplish.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes modifications to CIP-005 should be limited to conforming changes only.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT maintains modifications are necessary for CIP-010 and has not limited proposed modifications to conforming changes. The SDT focused more on objective type language versus a prescriptive list. At this time, the SDT does not plan to separate virtualization requirements from the existing requirements. Project 2016-02 is not just about enabling the CIP Standards for virtualization and opening the toolbox for this option, but rather to remove encumbrances while maintaining security and backwards compatibility as key objectives. The existing baseline attributes are administratively burdensome and serve as a disincentive to virtualize, even where virtualized solutions may be more secure. Additionally, the existing construct does not lend well to a virtualized environment. The proposed modifications shift the focus from a documentation burden to security value by requiring the authorization of change instead of the update of documentation 30 calendar days after a change. The order of operations may also be different in a virtualized environment, requiring adjustments to Requirement R1, which seems to prescribe an order of 1) identify security risk, 2) authorize, 3) implement, 4) verify, remediate, reverify. For example, in a virtualized environment using Remediation VLANs the order might be 1) authorize, 2) identify security risk, 3) remediate and verify, 4) implement; without modifications entities may not be able to use features like Remediation VLANs. The prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement with 'baselines' as one means to achieve the objective. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. The purpose is to add clarity that an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...". The changes then require authorization per Requirement R1 Part 1.1, and which changes to high impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA, and SCI supporting an Applicable System in Requirement R2 Part 2.1 are then subject to the monitoring requirements in Requirement R2 Part 2.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way how an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear. Additional rationale and use case examples for these changes can also be found in the TR.	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
There is insufficient clarity provided within the proposed terms to ensure consistent understanding and implementation of “Management Interface”. See response to #2 above.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDTreworded R1.3 around Management Interfaces to be more objective.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA does not support the expansion of R1, Part 1.6 to include the protection of data traversing communications links. Expansion to communications links does not consider devices that cannot meet this criterion. Putting communication links in scope would increase costs and maintenance activities, and would require re-architecture of links. Additionally, Exemption 4.2.3.3 maintains the communications exemption for the equipment on the communications link in a ‘super-ESP’, whereas an encryption requirement when traversing multiple geographic locations would increase security for these super-ESPs. BPA suggests reverting to the Draft 3 language for R1, Part 1.6. BPA does not agree with the requirement to mitigate risk represented by sharing memory resources in R2, Part 2.6.1. The theoretical risk represented by CPU-sharing is not high enough to mandate the significant re-architecture required to adequately separate CPU usage as specified in Part 2.6.1. BPA recommends allowing the continued use of shared resources to allow entities the flexibility to balance risk mitigation with resources, maintenance and cost of maintaining the grid.	
Likes 0	
Dislikes 0	

Response
Thank you for your response. 1.6 The SDT feels the objective for the level of protection in the requirement is appropriate. This covers expansion of an ESP outside of a PSP or between sites (Super ESP). The requirement language is worded to be backwards compatible with approved versions of CIP-006 R1.10. The proposed Exemption 4.2.3.3 is for equipment "between" the devices providing encryption, not for the devices themselves. 2.6.1 Now 2.6 -The SDT modified the Intermediate System affinity requirement to "Not share CPU or memory resources with any part of a high or medium impact BCS."

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	No
Document Name	

Comment
CIP-005 R1.2 does not state that there must be a justification for the need of routable protocol communication except for in the Measures column. We recommend the SDT change the wording from permit only needed routable protocol communications, and deny all other routable protocol communications “through the ESP” to “into identified ESP(s).” ERC is defined as external routable ***connectivity***, but the requirement is for external routable ***communications***. This is another instance of the inconsistent use of routable protocol qualifiers. In the Measures column of CIP-005 R1.2, the Measure “Physical isolation of an ESP,” is confusing. The need to use routable “protocol” communications in the CIP-005 requirements is confusing. It makes it sound like routable ***protocol*** communications is something different than routable communications. You cannot have routable communications without a routable protocol unless you encapsulate the non-routable protocol. This current wording may support excluding serial communications that are encapsulated and transported via a routable protocol. It would be less ambiguous if the SDT drops the word “protocol” from routable protocol communications and just used “routable communications.”

For CIP-005 R1.5, we recommend the SDT add a “except during CIP Exceptional Circumstances” clause to the requirement (similar to the clause added to CIP-004 R3.5). There can be multiple single points of failure impacting the ability to detect known or suspected malicious IP communications. A logging server, line card, power source, management console or SIEM could fail resulting in an immediate potential instance of non-compliance. Many of these solutions require port mirroring and there are limitations to mirroring the same source networks to multiple destination interfaces. This creates a scenario where a failed patch or unexpected hardware failure would immediately result in a potential instance of non-compliance creating unnecessary administrative burden. One solution to solve this would be to use a SPAN aggregator that splits the SPANS to two different security devices (like an IDP), but this too creates a single point of failure that during a patch, reboot or any system failure, would automatically result in a potential instance of non-compliance. For CIP-005 R2.1, the SDT should change the requirement so that the Interactive Remote Access is only initiated ***from*** an intermediate System instead of ***through*** an Intermediate System so that it’s clear that encrypted communication stops at the Intermediate System and new communication is then established from the Intermediate System.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. R1.2 The SDT agrees and changed the requirement wording to add justification of need. The SDT cleaned up the use of "routable protocol" to be more consistent. Refer to Technical Rationale for further explanations. R1.2 The SDT agrees and removed "physical isolation" from the measures. R1.5 The proposed change is not within the SAR for this project. R2.1 The SDT feels that "through" an Intermediate System is more appropriate than "from" an Intermediate System as the latter implies that IRA can originate from the Intermediate System itself.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	

WEC Energy Group does not agree with the proposed edits in R1 as it references the new "Management Interface" definition of which we do not agree (see #2 response). We also note that the reference to the Electronic Access Point has been removed from the Applicable Systems column. The Electronic Access Point modified definition is suitable for referencing physical and virtual assets. Proposing the SDT leaves Electronic Access Point in the Applicable Systems column.

WEC Energy Group can support the proposed edits in R2 and R3.

Likes 0

Dislikes 0

Response

Thank you for your comments. R1.2 EAP - The SDT feels that ESP used within the requirement is proof of changes in technology such as zero trust. In a zero trust situation, the use of EAP would require the entity to document all internal ESP communications as every system would have its own EAP.

Kristine Martz - Amazon Web Services - 7

Answer	No
Document Name	

Comment

Regarding CIP-005 Part 1.4, AWS suggests not limiting authentication requirements to dial-up connections. The SDT should broaden this requirement to include other technologies (i.e. 4G, 5G, etc.). Limiting this requirement to dial-up only may inadvertently create a security gap where alternative connection methods are not required to authenticate.

Likes 0

Dislikes 0

Response

Thank you for your response. This is outside the scope of this project’s SAR.

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

There is still a gap between what is system-to-system and what is Interactive Remote Access (IRA) with the new IRA definition. Entities often rely on IRA ports for system-to-system communication but have not enforced protections to ensure that malicious actors do not use the ports – regardless of whether a remote access client is available or used. Additional technical measures or controls should be added to the Standard to ensure validity of communications to Applicable Systems.

CIP-005-8 depends upon approved SCI terminology and other definitions associated with virtualization. Approval of CIP-005-8 would be conditional, based upon approval of the entire suite of new standards associated with virtualization.

There is a significant concern is that an entity could implement "logical isolation" using only a host-based firewall on essential systems that are directly connected to the internet. Thus, exposing them to greater risk as compared the requirements in place today using defense-in-depth.

Further, introducing Shared Cyber Infrastructure (SCI) increases the number of Requirements and Parts that a Responsible Entity needs to track compared to simply identifying the hypervisor and associated hardware and "high-water-marking" them with the highest identified impact rating and creating a BCS. Allowing "mixed-trust" environments within the same SCI (hypervisor) increases the complexity and management of the environment as the SDT relaxes the "high-water-marking" required to this point. In addition, complex environments are permitted where both ESP and non-ESP Cyber Assets can be commingled on the same hardware using nothing more than affinity rules and virtual networking to segregate these systems. The complexity surrounding these installations could allow for increased risks from configuration mistakes such that ESPs could contain Intermediate Systems.

Finally, there is no NERC definition of "Remediation VLAN" so therefore the Responsible Entity could keep VMs spun up and within the Remediation network for extended periods of time – without the benefit of protections from the other CIP Standards. Accidental connection to production networks before these VMs has been properly remediated could lead to security issues and introduction of malicious communications.

CIP-005 Requirement R1 Part 1.6 – to protect the confidentiality and integrity of data traversing communication links that span multiple Physical Security Perimeters, does not carry a minimum level of encryption to be required. This could result in older less secure methods being used for connections leaving the data at risk. References to NIST documentation regarding minimum encryption is suggested. Further, dependence on third-party carriers to create the "super ESP" could allow encrypt-decrypt-encrypt situations that could jeopardize the required protections for confidentiality and integrity of the data.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

R2.1 The SDT feels the proposed IRA definition has enough content to clearly show that IRA must be user initiated and is not part of system to system process communications. Any system to system process communications utilizing the same network ports as IRA would not fall within the definition of IRA. The word "authorize" has been removed.

Definitions vs. Standards - The SDT has determined that for draft 5, changes made to the definitions from draft 4 will only affect the standards being re-balloted in draft 5. This concern will be addressed during the next webinar.

Logical isolation and Host based firewalls - The SDT crafted the language in such a way that the requirements are compatible with zero-trust type implementations, which implies all external type communications is untrusted. It will be difficult for an entity to meet all the requirements using traditional host based firewalls as they which are not centrally controlled / administered.

Remediation VLAN - The SDT crafted the requirements to be compatible with additional other methods than solely remediation VLANs.

SCI / Mixed usage - The SDT feels that the methodology around the requirements for SCI are crafted in order to be flexible as technology evolves such as zero trust.

R1.6 The SDT crafted a technical objective requirement to protect confidentiality and integrity and feels that using outdated encryption methods does not meet the objective. Also, exemption 4.2.3.3 is crafted so that R1.6 must be under an entity’s control even if a third party is being used.

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3

Recommend update to Part 2.1. Remove “authorized” from “Permit authorized.”

Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

1.2 The SDT does not consider "per system capability" appropriate, but excluded time sensitive communications. Regarding 1.3, not all Management Interfaces have this capability, so "per system capability" was deemed appropriate.

2.1 The SDT removed "authorize".

R2.6 The SDT redrafted requirement 2.6 (now 2.6 and 2.7) to be more Like CIP-007 R 1.3.

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3
Recommend update to Part 2.1. Remove “authorized” from “Permit authorized.”
Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

R1.2 The SDT does not consider "per system capability" appropriate.

R1.3 Not all Management Interfaces have this capability, so "per system capability" was deemed appropriate.

2.1 The SDT removed "authorize".

R2.6 The SDT redrafted requirement 2.6 (now 2.6 and 2.7) to be more Like CIP-007 R 1.3

Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC

Answer	No

Document Name	
Comment	
Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3 Recommend update to Part 2.1. Remove “authorized” from “Permit authorized.” Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. R1.2 The SDT does not consider "per system capability" appropriate. R1.3 Not all Management Interfaces have this capability, so "per system capability" was deemed appropriate. 2.1 The SDT removed "authorize". R2.6 The SDT redrafted requirement 2.6 (now 2.6 and 2.7) to be more Like CIP-007 R 1.3	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No
Document Name	
Comment	
Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3 Recommend an update to Part 2.1. Remove “authorized” from “Permit authorized.” Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments . R1.2 The SDT does not consider "per system capability" appropriate. R1.3 Not all Management Interfaces have this capability, so "per system capability" was deemed appropriate. 2.1 The SDT removed "authorize". R2.6 The SDT redrafted requirement 2.6 (now 2.6 and 2.7) to be more Like CIP-007 R 1.3	
John Galloway – John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
Request CIP-005 intermediate systems use a similar format to CIP-007 R1 Part 1.3. Recommend update to Part 2.1. Remove “authorized” from “Permit authorized.” Request clarification on why Part 1.3 includes “per system capability” and Part 1.2 does not.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. R1.2 The SDT does not consider "per system capability" appropriate. R1.3 Not all Management Interfaces have this capability, so "per system capability" was deemed appropriate.	

2.1 The SDT removed "authorize". R2.6 The SDT redrafted requirement 2.6 (now 2.6 and 2.7) to be more Like CIP-007 R 1.3	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	2016-02_Virtualization_Unofficial_Comment_Form.docx
Comment	
GSOC requests the SDT remove references to previous requirements regarding applicable systems and instead include the content in directly with regards to applicable systems in parts 2.2, 2.3, and 2.6. In requirement 1.6, GSOC recommends allowing for the use of a combination of both physical and encryption controls at the discretion of the responsible entity for protections in the same manner as is allowed in CIP-012 standards. {C}[TK1]{C} This inclusion of physically security controls will provide more latitude for the entity to increase security while still remaining compliant rather than relying solely upon either physical or confidentiality and integrity controls. GSOC recommends using “Confidentiality and integrity controls, and/or”, or an additional bullet point specifically allowing for a combination of confidentiality and integrity controls along with physical controls. In requirement 2.1, specifying ‘authorized IRA’ implies that all IRA must be authorized, i.e. enumerated and documented. Additionally, the 2.1 measures then require all IRA be routed through an Intermediate System, suggesting even unauthorized IRA must do so as well. This issue persists in 2.3. Requirement 2.5, 3.1, and 3.2 language on applicability should explicitly specify it applies to only SCI having vendor remote access, rather than every SCI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. R1.6 The SDT feels that the first bullet is objective and allows for either physical or logical protection. The second bullet for backwards compatibility purposes with the previous CIP-006 standards has been added. This gives the entity the option of using either bullet.	

R2.1 The SDT removed "authorized". R2.4/2.5/3.1/3.2 The SDT agrees to restore the approved applicability. 2.6.1 – Now 2.6 -The SDT modified the Intermediate System affinity requirement to “Not share CPU or memory resources with any part of a high or medium impact BCS.”	
Monika Montez – California ISO – 2 – WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	No
Document Name	
Comment	
The SRC suggests that IRA definition should remain unchanged and have the specific scenarios that these definition changes are attempting to address become part of the standard requirement language. (i.e. CIP-005-8 R2).	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The changes to the IRA definition are required to meet the objectives of the SAR. Requirement type language has been removed from the definition and placed within the R2 requirements	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Tri-State mostly agrees with the definition but thinks the second bullet,"Communication that originates from an Intermediate System"under what "IRA is not" is confusing. Isn't that system to system communication?	
Likes 0	
Dislikes 0	

Response	
Thank you for your response. The SDT cleaned up the definition for IRA. The purpose "Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs" is to exempt Cyber Systems that are already within an ESP	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS would like clarification on the restriction in R2.6.2. The part could be interpreted to restrict routable communication to any other devices or to restrict communication to those specific devices through an ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT revised R2.6.2 (now 2.7) and reworded it for clarity.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying CIP-005 to allow for more flexibility in implementing future technologies while maintaining and even increasing security.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, and support. See response to EEI.	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the proposed modifications to CIP-005	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Manitoba Hydro agrees with the direction of the standard drafting team. Additional clarity could be added to sub-requirement R2.4 and R2.5. The term “with vendor remote access” has been added to the “applicable system” column. The addition of “SCI supporting an Applicable System in this Part” could mean that vendor remote access to the SCI is not in scope if there is no vendor remote access to BCS, since there are two qualifiers. Manitoba Hydro suggests adding a the qualifier “Where vendor remote access is implemented,” to the “requirements” column similar to the change done for R1.4 for Dial Up access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT agrees and reverted the language back to what was previously approved.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	

Answer	Yes
Document Name	
Comment	
Chelan appreciates the SDT's work on IRA and CIP-005 and approves the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	

Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the revisions made to CIP-005 in Draft #4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the revisions made to CIP-005 for Draft 4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
William Steiner - Midwest Reliability Organization - 10	

Answer	Yes
Document Name	
Comment	

Part 1.5 – SCI is not afforded malicious communications protections like the other CA types. While we understand the desire to avoid monitoring heavy traffic like fiber-channel, there is still a real risk of malicious code over the network to/from hypervisors (and likely other SCI)

Part 1.6 – Communication between geographically dispersed SCI is not applicable, thus not necessarily afforded similar protections.

Part 1.6 - Including the 'Internet Protocol' qualification in the requirement could inhibit malicious communication detection for future technologies and implementations that may not use a traditional firewall and IP routing. In particular with the change from firewalls as the outer perimeter to a zero-trust implementation, there will likely be more configuration points that aren't also acting as routers, so the inherent protection from non-IP protocols offered by the separation of subnets will no longer be there and other protocols could pass.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments.

R1.5 The SDT has not included SCI in the Applicable Systems as it will likely be used to meet this requirement and could result in a "hall of mirrors".

R1.5 The SDT made this requirement more consistent by specifying "routable protocol" and will limit communications to routable protocol at this time so that other data center protocols currently in use are not inadvertently included.

R1.6 The SDT chose not to include SCI within the Applicable Systems as SCI itself may be used to provide the required protections . This may result in a gap in protection is certain situations, however the SDT feels that a majority of situations will be covered.

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	
Comment	

Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See response to EEI.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
BC Hydro agrres with the proposed changes; however, clarification is needed as follows: In CIP-005-8 Requirement 2.1 which is, "Permit authorized....". The use of the word "authorized" is creating confusion. Typically IRA through the Intermediate System is already authorized through CIP-004. SCI was already added into CIP-004 scope therefore SCI access is authorized. IRA is applicable to all asset classifications on top of SCI which is also authorized through the CIP-004 process and not at the intermediate system. BC Hydro kindly requests that the drafting clarifies the use of the term "authorized" and recommends that the drafting team consider removing the word "authorized" from the wording of Requirement 2.1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT removed the word "authorize".	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE is concerned the definitions of Cyber Asset and PCA introduce security risks in CIP-005. The definition of Cyber Asset explicitly excludes SCI from its definition, which means SCI cannot be a Cyber Asset. The definition of PCA explicitly includes Cyber Assets or Virtual Cyber Assets in the definition. SCI cannot meet either definition, which means a hypervisor cannot be dual categorized as SCI and PCA. Therefore, an SCI placed within a network protected by an ESP arguably would not be subject to CIP-005 R1.1, R1.2, R1.5, or R1.6 despite being a PCA in all but definition.

In addition, Texas RE notes that SCI supporting high and medium impact BCS have fewer network-based protections than high and medium impact BCS. CIP-005 R1.2 is applicable to high and medium impact BCS with ERC. The requirement requires that only needed routable protocol communications are permitted through the ESP. CIP-005 R1.3 is applicable to SCI supporting medium and high impact BCS. The requirement requires that only needed routable protocol communications to and from the Management Interfaces are permitted.

Additionally, Texas RE is concerned there may be means of communicating with SCI outside of the narrow scope of the Management Interface definition. For example, an FTP server would not control the process of initializing, deploying, or configuring SCI. An FTP server is not an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, or OS. Finally, an FTP server does not configure an ESP. As such, an FTP server running on SCI would be out of scope for CIP-005 R1.3. An FTP server in this scenario could be used to exfiltrate sensitive data, such as the disk images for the BCS that the SCI is hosting. Additionally, since SCI is out of scope for CIP-005 R1.5 entities would not be required to monitor this FTP server for malicious communications between the SCI and other systems. Texas RE suggests this issue would be mitigated by implementing high watermarking practices as described in Texas RE's response in #9.

Lastly, Texas RE continues to be concerned the security objective for CIP-005-6 R1 Part 1.5 is now limited to IP malicious communications with the proposed changes. With the proposed changes this would not only reduce the compliance obligations but also create a gap in security by only focusing IP malicious communications versus all malicious communications.

Likes 0	
Dislikes 0	

Response

Thank you for your response.

The SDT feels the option of mixed trust usage of SCI should be allowed as long as the appropriate protections are in place.

Definitions - The SDT chose to separate SCI from the definitions of CA, VCA, PCA and target separate specific protections on the SCI itself. This ensures the appropriate protections are placed for the applicable CA, VCA and PCA that are running on the applicable SCI, while allowing mixed trust to exist.

R1.1/1.2 - SCI may be utilized to provide network controls for the applicable systems in a zero trust environment, thus making SCI an applicable system would introduce a "hall of mirrors" issue.

R1.3 The requirement language around Management Interface was updated to be more objective.

R1.5 The SDT feels that limiting malicious communications monitoring to IP communications is appropriate. IT is including other internal data center communications currently in use such as high fiber channel SAN cannot be monitored.

R1.5/1.6 The SDT reviewed whether it was appropriate to add SCI to R1.5 or 1.6, however SCI could be used to meet both these requirements, thus a "hall of mirrors" issue would be introduced.

FTP/BCSI - Disk images of applicable systems are considered BCSI and should be protected as such. BCSI storage is currently allowed outside of an ESP. The SDT notes that some issues around FTP could currently exist and are not SCI related. FTP remote user interactive communications are covered by the requirements around IRA and non-user interactive communications are covered under system to system process communications.

Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	

4. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)

Answer	No
Document Name	

Comment

The SRC agrees with the concept of per system capability.

For Part 1.3, we recommend changing "prevention" to "risk mitigation". "Preventing" is absolute. "Risk mitigation" is flexible.

For Part 4.3, we request adding "security" to "applicable events" for consistency with Parts of R4. Update would read "Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances."

For Part 4.4, please consider rewording this requirement to accommodate entities that use the current SIEM technology which has this type of functionality built-in and no longer requires a manual review of such data sources while also addressing those that do not have this technology.

For Part 5.1 and 5.4, leaving the scope of the term "system" up to the entity, requires effort to supply a definition and document compliance with the definition. This could lead to a misunderstanding of the intent of that term. We recommend that SDT update the technical rationale to include what is meant by "system".

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT updated the wording of the requirement and added more clarification to the technical rationale. Additionally, the terminology was made more consistent and 4.3 was clarified to reflect application security events. The change to 4.4 is out of scope of the SAR for Project 2016-02.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No

Document Name	
Comment	
No, 1.3 requirement is written more like measure with the word prevent. Would suggest rewording it to "Mitigate VCA's from CPU or memory vulnerabilities that share these resources with other VCA's that are not associated with the same impact categorization." Then prevention could be one of the measures.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement and added more clarification to the technical rationale.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	
For Part 1.3, recommend changing “prevention” to “risk mitigation.”“Prevention” is absolute. “Risk mitigation” is flexible. Perhaps “prevention” can be moved to the Measures as a suggestion/ Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles. For Part 4.3, request adding “security” to “applicable event” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT clarified the wording of the requirement and added more clarification to the TR. The terminology was made more consistent and 4.3 was updated to reflect application security events.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	

Answer	No
Document Name	
Comment	

For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion.

Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles.

For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. The update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT clarified the wording of the requirement and added more clarification to the TR. The terminology was made more consistent and 4.3 was updated to reflect application security events.

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	
Comment	

In R1.1, Ameren believes that the phrase "routable protocol network accessibility" is unclear and there should be more clarity as to what this phrase means. We are concerned an auditor might think of this phrase differently than Ameren does, so we believe more clarity around this phrase will ensure that auditors and Ameren have the same understanding as to what the phrase means.

In R4.3, the phrase "per system capability" was added. Does any paperwork need to be filled out and provided to the regional entity for devices that fall into the "per system capability" classification? For example, paperwork needs to be filled out for TFEs.

Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT added clarity in the TR for both the phrase "routable protocol network accessibility" in 1.1 and "per system capability" in 4.3.	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	No
Document Name	
Comment	
For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion. Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles. For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement and added more clarification to the TR. The terminology was made more consistent and 4.3 was clarified to reflect application security events.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion. Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles.	

For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement and added more clarification to the TR. The terminology was made more consistent and 4.3 was clarified to reflect application security events.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
For Part 1.3, recommend changing “prevention” to “risk mitigation”. “Preventing” is absolute. “Risk mitigation” is flexible. Perhaps prevention can be moved to the Measures as a suggestion. Request consistent phrasing in CIP-007. There is a mix of “cyber security patch” and “security patch” in the Parts, Requirements, and titles. For Part 4.3, request adding “security” to “applicable events” for consistency with Parts of R4. Update would read “Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement and added more clarification to the TR. The terminology was made more consistent and 4.3 was clarified to reflect application security events.	
Ronald Bender - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	

Recommend removing EACMS and PACS from the applicability section. If EACMS or PACS were to reside inside an ESP they are also categorized as PCAs so they will be covered. This change will exclude other CAs in a DMZ virtual system that do not perform EACMS or PACS functions and will thus retain the backward compatibility of the standard while allow greater protection for BCAs and PCAs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement, removing EACMS and PACS.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	No
Document Name	
Comment	
Chelan believes the proposed language for CIP-007 R1.3 is overly burdensome and the required control does not reflect the actual risk of a VM escape attack. The intended controls (DRS affinity rules) listed in the measures are not intended for security control purposes, but are instead intended for resource control purposes. Because of this and the very broad applicability, they will have overly complex rulesets that introduce reliability risks where, in the event of a failure or during maintenance activities, a crucial VM may not be able to find a suitable host and crash. Given there are few if any demonstrated attacks along this threat axis, this seems to be an overreach. Additionally, this requirement is not backwards compatible with the existing requirements. The currently effective requirements allow the mixing of EACMS and PACS VMs with out-of-scope VMs so long as the hosts themselves are classified as EACMS and PACS. Finally, Chelan believes there is a Low Impact problem in the proposed requirement. The Applicable System is an SCI that hosts High or Medium Impact VCAs, not the actual High or Medium Impact VCAs themselves. The text of the requirement itself does not restrict itself to High and Medium and simply refers to “same impact classification”. If an SCI that hosts High or Medium Impact VCAs also hosts Low Impact BCS, the requirement is on the SCI to prevent sharing of CPU and memory between devices that are not of the same impact categorization, regardless of what that impact categorization might be. Low Impact is a different impact category from no impact, so the requirement would force the SCI to segregate Low Impact VCAs from no impact VCAs. That essentially places a requirement on Low Impact devices to not share CPU and memory with no-impact devices, so long as they are on the same SCI as a High and Medium impact VCA. All that said, Chelan does recognize the risk of a zero day exploit along this vector and therefore, Chelan recommends this requirement should be restricted to BCAs and PCAs, and left EACMS and PACS out, which would be backwards compatible with the existing requirements and guidance. The	

suggested language below would prevent devices that are within the ESP from sharing CPU and memory with devices outside the ESP or in different impact level ESPs. This would accomplish the goal of protecting BES Cyber Systems and would simplify implementation by creating three categories of devices that may not share CPU and memory, rather than potentially six. Chelan suggests the following language for CIP-007 R1.3: Applicable Systems: SCI supporting: High Impact BCS and their associated PCA; Medium Impact BCS and their associated PCA Requirement: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources, excluding storage resources, between High and Medium Impact BCS and their associated PCA, and VCAs that are not BCS or PCAs of the same impact categorization.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT updated the wording of the requirement, removing EACMS and PACS.	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group does not agree with the proposed edits and retitling of R1. Changing the title of R1 to System Hardening implies the potential for more than just the management/monitoring of ports and services. Although "system hardening" is a best practice, it is at this time self defined and is too broad of a term to be used for CIP-007 R1 and in our opinion beyond the virtualization intent of the Project. Additionally, Part 1.1 implies ports and services in the Requirement, we understand it was rewritten in an attempt to address SCI supporting the Applicable System, however the rewrite is too broad and looses its intent of ports and services. Also note, the Measures for Part 1.1 describes the aspects of ports and services, why not use those same terms (ports and services) in the Requirement itself. Proposing the SDT leaves the title of the R1 as Ports and Services, leave R1 Part 1.1 and Part 1.2 as written and separate the SCI references included in current draft Part 1.3 into its own Requirment or Part. WEC Energy Group can support the proposed edits in R2-R5.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The reasoning behind the name change is to reflect the security objective of the entries more clearly in the table, which is to reduce a systems' attack surface. The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCA.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
As it pertains to CIP-007 R4.2, the use of the term system in the statement "per system capability" leads to subjectivity. We recommend the use of "per Cyber Asset or BSC capability" as it defines the scope of capability. Additionally, our comment from the last comment period of "If a firewall has VLANs on it for medium and low, or high and low, does that pull low impact network connection into scope because it shares the same firewall?" was not addressed by SDT as far as we know.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT added more clarification to the TR.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes modifications to CIP-007 should be limited to conforming changes only.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. The SDT is changing R1.1 so that it can incorporate newer security models, such as zero trust. The addition of R1.3 addresses the possibility of VM escape. Refer to the CIP-007-7 TR for more information	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern disagrees with the proposed changes to CIP-007 R1.3 Applicable Systems. Adding EACMS and PACS in both High and Medium Impact BCS increases the requirements for associated virtual assets. Southern agrees that for hypervisors which ALSO host BCS, the scope is appropriate, but for hypervisors that ONLY host EACMS outside of an ESP, with no BCS, it is an “anti-virtualization” incentive to dedicate hypervisors to a domain controller for example. Suggest changing the language to High/Medium Impact BCS and their associated PCA, which will keep this affinity requirement scoped to hypervisors that host BCS and anything else.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT clarified the wording of the requirement, removing EACMS and PACS.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	

See response to EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the revisions made to CIP-007 for Draft 4.	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
AEP supports the revisions made to CIP-007 in Draft #4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	

Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the proposed modifications to CIP-007.	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying CIP-007 to allow for more flexibility in implementing future technologies while maintaining and even increasing security.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See the response to EEI.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the revised CIP-007 proposed changes.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	
Comment	
Texas RE is concerned the language: “logical network accessible ports… including port ranges or services where needed to handle dynamic ports” was removed. Both ports and services are required to gain a better understanding of where vulnerabilities can exist whether in a physical or virtualized environment. Ports and services are often used for malicious reconnaissance and lateral movement within networks. Registered Entities should understand and document why ports and services are needed for many reasons (defense in depth, zero trust, etc. concepts). Texas RE is concerned the phrase “CPU and memory resources” in CIP-007-7 Requirement R1.3 is written could be interpreted as (CPU and memory) resources or as CPU and (memory resources). Texas RE recommends rewording the sentence so it is clear that the CPU resources and memory resources should not be shared: “the sharing of CPU resources and memory resources.” Additionally, in order to make the language of Requirement 1.3 more consistent with other requirements in CIP-007-7, Texas RE recommends revising the existing language Requirement R1.3 to “Prevent the sharing of CPU resources and memory resources, excluding storage resources, between Virtual Cyber Assets (VCAs) that are not of, or associated with, the same impact categorization.” The technical rationale for this requirement can then explain that the requirement is needed in order to mitigate the risk of CPU or memory vulnerabilities. Lastly, Texas RE noticed inconsistent redlining between the “redline_to_last_approved” and “clean” copies of the standard for CIP-007-7 R4.1. In the “clean” version of the standards the following language, which Texas RE agrees with reads as: Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events In the “Redline to Last Approved” version the phrase “and after-the-fact investigations of” has been marked for removal. Texas RE does not agree with removing this phrase from the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT clarified the wording in 1.3 and 4.1. The phrase "after-the-fact investigations of" has not been removed.	

5. The SDT has used phrasing such as "SCI supporting an Applicable System from this Part" in the Applicable Systems column across many of the standards. Is it clear that this scopes the requirements for SCI to match the system(s) it hosts?	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes the phrase needs to be more specific. "Supporting" an Applicable System is too broad. BPA proposes adding SCI under the Applicable Systems column in the Requirements/Parts tables, grouping it with each appropriate impact rating similar to the way EACMS, PACS, and PCA are scoped. Additionally, the definitions for EACMS and PACS include SCI so these do not need to be accounted for. Alternatively, since the term "and their associated" is widely used in the standards, replacing the word supporting with "associated with" may be more clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT believes the use of "SCI supporting an Applicable System from this Part" in the Applicable Systems column of the requirement, to ensure that controls relevant to the hardware portion of a physical Cyber Asset, would remain applicable to the hardware supporting the VCA used in BCS, EACMS, PACS or PCA. Clarifying updates have been added to the TR.	
Israel Perez - Salt River Project - 6	
Answer	No
Document Name	
Comment	
The phrase "SCI supporting an Applicable System from this part" is still not clear enough and needs more verbage to explain what it applies to. The phrase could also be re-written as "SCI supporting the identified Applicable System in this Part"	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT believes the use of "SCI supporting an Applicable System from this Part” in the Applicable Systems column of the requirement to ensure that controls applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA. Additional clarity has been added to the TR.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
"Part" is not a defined term, for additional clarity the drafting team could replace this phrase with "SCI supporting an Applicable System". Lastly, "Applicable System" is used multiple times in the draft CIP standards and is not a defined term or a proposed defined term. The standard drafting team may consider defining this term in the NERC Glossary of Defined Terms.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. “Part”, “Applicable System”, “Requirements”, and “Measures” are used throughout the CIP standards, in both verbiage and in the table column titles. The SDT does not find it necessary to add these to the NERC Glossary.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No, Supporting an applicable system is not specific enough and could be misterupted	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment. The SDT believes the use of "SCI supporting an Applicable System from this Part" in the Applicable Systems column of the requirement to ensure that controls applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA. Additional clarity has been added to the Technical Rationale.	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees and appreciates the included language of “SCI supporting an Applicable System in this Part” across the many standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes

Document Name	
Comment	
AZPS agrees that the phrasing of “SCI supporting an Applicable System from this Part” is clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy believes there is some lack of understanding at our company and throughout the industry on how SCI should be categorized when they are supporting EACMS or PACS and so, Xcel Energy supports the comments of the MRO NSRF. While Xcel Energy supports clarifications, our concerns do not rise to the level of requiring us to vote no on proposed Standards with SCI as an applicable system.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. SCI is much like EACMS and PACS in that these categories of Cyber Assets do not technically have a direct impact rating, making their categorization less conducive to ‘high watermarking concepts.’ Where SCI supports EACMS and PACS (and not BCS or PCA), the SCI inherits the requirements for the collective impact ratings of each associated BCS for each of the EACMS and PACS that SCI supports. Registered Entities implementing SCI that supports both EACMS and PACS should approach categorization holistically and apply multiple categorizations and collective coverage of that supporting SCI under all applicable Requirement Parts. Registered Entities run the risk of security/compliance gaps if attempting to ‘high watermark’ to a single categorization where SCI supports both EACMS and PACS associated to varied impact levels of BCS. The applicable requirements are an aggregate of the requirements of the hosted	

Applicable Systems. See the TR for a more comprehensive explanation, including an example of a specific use case.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees the phrasing of “SCI supporting an Applicable System from this Part” in the Applicable Systems column in the Standards makes it clear the scoping is for the hosts the SCI supports.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	

Answer	Yes
Document Name	
Comment	
This is fairly clear. However it would be better to see some verbiage/examples in the technical rationale related to the inclusion of “storage resources required for system functionality of one or more Cyber Assets or VCAs….” found in the second bullet of the SCI definition to limit the scope of applicability. It’s not quite clear what exactly may be pulled into scope by the wording in the second bullet and there may be an unintentional increase in applicability. CIP-007 R1.3 specifically excludes storage resources in the requirement, but in the definition of SCI, the second bullet specifically includes storage resources in the definition of SCI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. See the TR for CIP-007 R1.3 for additional clarification.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes

Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the phrasing “SCI supporting an Applicable System from this Part” in the Applicable Systems column across many of the standards is clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	

Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	

6. The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Larry Heckert - Alliant Energy Corporation Services, Inc. - 4

Answer	No
Document Name	

Comment

Alliant Energy supports the comments submitted by the MRO NSRF

Likes 0	
Dislikes 0	

Response

See response to MRO NSRF.

Daniel Gacek - Exelon - 1

Answer	No
Document Name	CIP-010 Alternate Update.docx

Comment

ecommending maintaining the CIP-010-4 requirement to establish and maintain the baseline.

Justification:

While the TR does allude to the use of the baseline configuration as the "how" this requirement can be met, it is followed by stating the entity would be required to document how the baseline meets the stated security objective and references NIST SP 800-128 as a guide.

Throughout NIST SP 800-128 the baseline configuration is referenced as the "secure state", specifically "…*baseline configuration for a system and associated components represents the most secure state consistent with operational requirements and constraints*" (NIST.SP.800-128, Section 2.2.2, pp. 21). Establishment and maintenance of a baseline configuration provides the entity with a secure starting point from which each modification can build upon.

Removing the requirement for a baseline configuration and/or requiring the entity to justify the use of the baseline appears to go against the guidance provided in NIST 800-128.

R1 Response

Part 1.1

R1.1 Document and maintain system configurations (to include at a minimum software addressing the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.)

R1.1.1 Manage changes which alter the system configuration

R1.1.2 Authorize changes to the system configuration

R1.1.3 Validate implementation of changes to the system configuration

Part 1.2

1.2.1. Prior to implementing a change to system configurations from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 andCIP-007 remain implemented as required; and

1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Part 1.3

For a change that deviates from the existing system configuration, update the system configuration documentation as necessary within 30 calendar days of completing the change.

R2 – Security Configuration Monitoring

Considering the changes made to R1 and the proposal to maintain the baseline configuration documentation requirements the following is a proposed adjustment to R1.

Response

Part 2.1

Methods to monitor at least once every 35 calendar days for unauthorized changes to the system configuration. Document and investigate detected unauthorized changes.

1 – The language used in the requirement, specifically “settings”, will force a significant and increasing administrative burden on the Entities. The control which applies to the requirement for each of the items within CIP-005 and CIP-007 will typically contain a multitude of “settings” which enforces the configuration of the control as a collective. There is a concern that the Entity will be ‘too far in the weeds’ focusing on the numerous settings that contribute to a control thereby diverting attention from the security posture of the environment.

2 – Confirmation after implementation of the authorized/documented change of the controls which enforces the requirement in CIP-005 and CIP-007 ensures the security configuration of the applicable system was not impacted in a manner that would weaken the security posture of the applicable system.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT considered the suggestion to reintroduce the word 'baseline' so R1 would provide clarity on 'how' to meet the requirement using a 'baseline'. It was determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. The SDT also maintains that the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility and provide clarity, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to demonstrate an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", and then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)

Answer	No
Document Name	

Comment

The proposed changes to CIP-010 are SRC's gravest concern as we believe the proposed changes go beyond what was previously in the CIP standards such that they would no longer be backwards compatible. In particular, the addition of the concept of "settings changes" is overly broad; whereas the prior standard focused on changes to the baseline configuration. SRC proposes "settings changes" be modified to "configuration changes" or eliminated altogether.

For consistency, please add the term "Cyber" to security patches.

The SRC requests clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document that baselines (from previously approved Standard) track or show any changes made to applicable CIP-005 and CIP-007 security controls

The SRC requests that consistent language be used when addressing the same subject in different parts of the standard within the Requirements of Parts 1.1 and 1.3. Examples of this include the following:

- *Part 1.1 provides what is included in software*
- *Part 1.3 distinguishes some of 1.1 apart from software*
- *Part 1.1 starts with "Control the implementation of intended changes to software, or intended changes to settings . . ."*
- *Part 1.1 also says "Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.*
- *Part 1.3 starts with "Prior to the installation of operating systems, firmware, software, or software patches . . ."*

While we recommend that that CIP-010 R1 needs to be left "as is" as changing the requirement may present a greater compliance burden on the entity with a less clear objective/goal. The proposed changes do not increase the level of security that are currently afforded by the existing standard.

For Part 2.1, we recommend this requirement is also left "as is". The proposed requirement is overly burdensome and may require the monitoring of the entire asset, including its filesystem, registry, miscellaneous settings, accounts, etc. and is above and beyond what is currently required with little added security benefit.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT considered comments regarding the potential for confusion, perceived scope increase, or misinterpretation by use of terms like "settings". This phrasing was removed to prevent it from being interpreted as too prescriptive.

The SDT agreed with suggestions to add the word "cyber' in front of "security patches", and updated the term throughout the standards.

Regarding the need for Measures to meet the Objectives and consistency of terms, and when modifying Requirement R1, the SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain a choice for an entity to demonstrate compliance, as well as assure the virtualization components are aligned. The TR was reviewed to ensure the baseline part is clear.

The SDT maintains Project 2016-02 is not just about enabling the CIP Standards for virtualization and opening the toolbox for this option, but rather the intention to remove encumbrances, while maintaining security and backwards compatibility as key objectives. The existing baseline attributes are administratively burdensome and serve as a disincentive to virtualize, even where virtualized solutions may be more secure. Additionally, the existing construct does not lend well to a virtualized environment. The proposed modifications shift the focus from a documentation burden to security value by requiring the authorization of change instead of the update of documentation 30 calendar days after a change. The order of operations may also be different in a virtualized environment, necessitating adjustments to Requirement R1, which seems to prescribe an order of 1) identify security risk, 2) authorize, 3) implement, 4) verify, remediate, reverify. For example, in a virtualized environment using Remediation VLANs, the order might be 1) authorize, 2) identify security risk, 3) remediate and verify, 4) implement; without modifications entities may not be able to use features like Remediation VLANs. The SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement with 'baselines' as one means to achieve the objective. The focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. To maintain backwards compatibility and clarity, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. This demonstrates an entity can continue to use baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement part(s) in CIP-005 or CIP-007...", which changes then require authorization per Requirement R1 Part 1.1, and which changes to high impact BES Cyber Systems and their associated 1. EACMS; and 2. PCA, and SCI supporting an Applicable System in Requirement R2 Part 2.1 are then subject to the monitoring requirements in Requirement R2 Part 2.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

R1.1 The phrase "...could weaken configured cyber security controls.." is very general and expands the original baseline scope widely to include endless settings that could be under the review of an audit.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT considered your perspective, agrees it carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	CIP-010 Alternate Update.docx

Comment

Recommending maintaining the CIP-010-4 requirement to establish and maintain the baseline.

Justification:

While the TR does allude to the use of the baseline configuration as the “how” this requirement can be met, it is followed by stating the entity would be required to document how the baseline meets the stated security objective and references NIST SP 800-128 as a guide.

Throughout NIST SP 800-128 the baseline configuration is referenced as the “secure state”, specifically “…*baseline configuration for a system and associated components represents the most secure state consistent with operational requirements and constraints*” (NIST.SP.800-128, Section 2.2.2, pp. 21). Establishment and maintenance of a baseline configuration provides the entity with a secure starting point from which each modification can build upon.

Removing the requirement for a baseline configuration and/or requiring the entity to justify the use of the baseline appears to go against the guidance provided in NIST 800-128.

R1 Response

Part 1.1

R1.1 Document and maintain system configurations (to include at a minimum software addressing the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.)

R1.1.1 Manage changes which alter the system configuration

R1.1.2 Authorize changes to the system configuration

R1.1.3 Validate implementation of changes to the system configuration

Part 1.2

1.2.1. Prior to implementing a change to system configurations from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 andCIP-007 remain implemented as required; and

1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Part 1.3

For a change that deviates from the existing system configuration, update the system configuration documentation as necessary within 30 calendar days of completing the change.

R2 – Security Configuration Monitoring

Considering the changes made to R1 and the proposal to maintain the baseline configuration documentation requirements the following is a proposed adjustment to R1.

Response

Part 2.1

Methods to monitor at least once every 35 calendar days for unauthorized changes to the system configuration. Document and investigate detected unauthorized changes.

1 – The language used in the requirement, specifically “settings”, will force a significant and increasing administrative burden on the Entities. The control which applies to the requirement for each of the items within CIP-005 and CIP-007 will typically contain a multitude of “settings” which enforces the configuration of the control as a collective. There is a concern that the Entity will be ‘too far in the weeds’ focusing on the numerous settings that contribute to a control thereby diverting attention from the security posture of the environment.

2 – Confirmation after implementation of the authorized/documented change of the controls which enforces the requirement in CIP-005 and CIP-007 ensures the security configuration of the applicable system was not impacted in a manner that would weaken the security posture of the applicable system.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT considered the suggestion to reintroduce the word 'baseline' so R1 would provide clarity on 'how' to meet the requirement using a 'baseline'. It was determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. Additionally, the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility and clarity, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to demonstrate an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement part(s) in CIP-005 or CIP-007...", and which changes then require authorization per Requirement R1 Part 1.1. The measures were aligned by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear.

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

R1.3 – consistency of phrases among the requirements is necessary, For instance, in Requirement 1 part 3, the phrase used is “Prior to installation.” In other sections, however, the phrase used is “prior to the intended change” One of the two phrases should be used throughout.

Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls.

Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to software, or intended changes to settings . . .” Part 1.1 also says “Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .”

For Part 3.3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term? “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s.

For Part 3.3, request removing “any” from the first Measures bullet because “any” is a scope concern where “any” is interpreted as “all.”

For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT was mindful to assure alignment of terms.

The SDT revisited the Measures when making modifications to Requirement R1 Part 1.1 to assure the Measures meet the Objectives of the requirements as suggested.

Also considered were comments regarding Requirement R3 Part 3.3, the phrasing 'Like replacements', and defining the term. Rather than introduce a new definition, the SDT made modifications to shift the focus on "previously assessed configuration" as the reason why an active vulnerability assessment need not be reperformed. The intent is to require assessments to reduce the risk of introducing vulnerabilities to an existing environment when new Cyber Assets are being implemented, or when failures occur and existing Cyber Assets need to be replaced. The risk is associated with unassessed configurations for these Cyber Assets. A 1-for-1 replacement of an existing Cyber Asset with another, configured like the one being replaced, suggests the security posture is known as a function of the reconstruction process to build the replacement. Since the existing Cyber Asset had been previously assessed, the performance of the requirement part is not warranted. Entities can still choose to define the term ‘like replacements’ within their own programs and processes if the Registered Entity deems that necessary or a value add.

The SDT removed the word "any" from the Measures for Requirement R3 Part 3.3 as requested.

Regarding Requirement R4, Attachment 1, Section 1, Part 1.3 and the risk associated with the new bullet that reads, “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;”, the SDT agrees with the unintended consequence that this may leave a gap where newer software vulnerabilities could exist for an earlier known state that have not been addressed. The bullet was removed in response to this industry concern.

Jennifer Wright - Sempra - San Diego Gas and Electric - 5

Answer	No
Document Name	
Comment	
The word "setting" should be further clarified.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Regarding the potential for confusion, or perceived scope increase or misinterpretation by use of terms like "settings", the SDT agreed this would be interpreted as too prescriptive and the phrasing was removed.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	

SPP would like to understand how the significant proposed changes in CIP-010-5, specifically Requirement R1, relate to what was requested in the Project 2016-02 SAR. SPP believes that the verbiage related to SCI, containerization, and ESPs between systems with different impact ratings can be added without having to change the way that entities have to comply with CIP-010 today.

The new proposed language greatly expands the scope for CIP-010 and raises concerns for backwards compatibility with existing baseline methods, adds unnecessary complexity, and significantly increases cost with minimal security benefit. The current baseline configuration requirements have been moved to the Measures column along with additional verbiage to address virtualization. However, the control language is very broad and can lead to different interpretations depending on the auditor and uncertainty in tracking changes. Responsible Entities have demonstrated that both physical and virtual systems are capable of developing, documenting, approving, tracking, updating, and monitoring baseline configurations. For these reasons, SPP believes that the prescribed baseline configuration requirements should remain in place with the addition of specific verbiage related to virtual architecture and containerization. The baseline language supports a secure baseline configuration and represents industry best security practices.

The NIST 800-128 guidelines refer to applying the security configuration management practices that include “monitoring the configuration of systems to ensure that configurations are not inadvertently altered from the approved baseline”, thus implying that baseline configuration management is key to securing a system. These guidelines further define a Baseline Configuration as, “A set of specifications for a system, or CI

within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes." This definition fits well with the currently approved verbiage in CIP-010-4 where the "set of specifications for a system" was clearly defined for the baseline and approved through change control methods. The baseline is an understanding of what the approved system configuration should be so that there is an understanding of what has changed. According to NIST, the baseline configuration should represent a secure state of the system while also maintaining a "cost-effective and functional support of mission and business processes". The updated control verbiage does not reference a baseline configuration and does not adhere to a cost-effective support of security best practices, therefore creating a risk to demonstrate compliance.

The following proposed language for CIP-010-5, Requirement R1, Part 1.1, could address virtualization while also maximizing backwards compatibility:

Develop a baseline configuration, individually or by group, which shall include the following items:

1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;

1.1.2. Any commercially available or open-source application software (including version)

intentionally installed including application containers;

1.1.3. Any custom software installed, including application containers;

1.1.4. Configuration that modifies network accessible logical ports or network accessible services on an Applicable System;

1.1.5. Any security patches applied;

1.1.6. SCI configuration of host affinity control between systems with different impact ratings;

1.1.7. Changes to configurations or settings for an ESP between systems with different impact ratings; and

1.1.8. Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT maintains Project 2016-02 is not just about enabling the CIP Standards for virtualization and opening the toolbox for this option, but rather the intention to remove encumbrances, while maintaining security and backwards compatibility as key objectives. The existing baseline attributes are administratively burdensome and serve as a disincentive to virtualize, even where virtualized solutions may be more secure. Additionally, the existing construct does not lend well to a virtualized environment. The proposed modifications shift the focus from a documentation burden to security value by requiring the authorization of change instead of the update of documentation 30 calendar days after a change. The order of operations may also be different in a virtualized environment, requiring adjustments to Requirement R1, which seems to prescribe an order of 1) identify security risk, 2) authorize, 3) implement, 4) verify, remediate, reverify. For example, in a virtualized environment using Remediation VLANs, the order might be 1) authorize, 2) identify security risk, 3) remediate and verify, 4) implement; without modifications entities may not be able to use features like Remediation VLANs. The SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement with 'baselines' as one means to achieve the objective. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. To maintain backwards compatibility and clarity, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to demonstrate an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement part(s) in CIP-005 or CIP-007...", which changes then require authorization per Requirement R1 Part 1.1, and which changes to high impact BES Cyber Systems and their associated 1. EACMS; and 2. PCA, and SCI supporting an Applicable System in Requirement R2 Part 2.1 are then subject to the monitoring requirements in Requirement R2 Part 2.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear, and additional examples of these changes can be found in the TR.

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF

Answer	No
Document Name	

Comment

While we appreciate the thoughtful proposal of a less prescriptive requirement for CIP-010, there are many unintended consequences with the expansion of scope in the currently proposed language. The word “settings” scopes too many possible features into CIP-010 that do not necessarily have a compelling security value. Additionally, the concept of a baseline is foundational in NIST SP 800-128 . It is possible to have less prescriptive requirements that advance the intention of CIP-010 and its security objectives,while maintaining true backward compatiability.Here is our alternate proposal that we have worked with Exelon to craft:

R1.1 Document and maintain system configurations (to include at a minimum software addressing the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.)

R1.1.1 Manage changes which alter the system configuration

R1.1.2 Authorize changes to the system configuration

R1.1.3 Validate implementation of changes to the system configuration

R1.2.1. Prior to implementing a change to system configurations from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 andCIP-007 remain implemented as required; and *R1.2.2. Document the results of the testing, and if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.* *R1.3 For a change that deviates from the existing system configuration, update the system configuration documentation as necessary within 30 calendar days of completing the change.* *R2.1 Methods to monitor at least once every 35 calendar days for unauthorized changes to the system configuration. Document and investigate detected unauthorized changes.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Regarding the potential for confusion, or perceived scope increase or misinterpretation by use of terms like "settings", the SDT agreed this would be interpreted as too prescriptive and the phrasing was removed. The SDT considered the suggestion to reintroduce the word 'baseline' so R1 would provide clarity on 'how' to meet the requirement using a 'baseline'. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. Additionally, the SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility and clarity, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to demonstrate an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", and which changes then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	No

Document Name	
Comment	
Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. The entity may need to document its baselines (from previously approved standards) when addressing its CIP-005 and CIP-007 security controls. Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in the software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to the software or intended changes to settings . . .” Part 1.1 also says “Changes to the software include the installation, removal, or update of the operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .” For Part 3.3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term? “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s. For Part 3.3, request removing “any” from the first Measures bullet because any is a scope concern . . . where any is interpreted as “all.” For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Regarding the need for Measures to meet the Objectives and consistency of terms, and when modifying Requirement R1, the SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance, as well as to assure the virtualization components are aligned. The TR was reviewed to ensure the baseline part is clear. The SDT made modifications to assure consistent use of terms instead of the use of similar terms like “software patches” and “security patches” to further remove any concerns of unintended nuances from using synonymous terms interchangeably; cyber security patches is now the term used throughout.	

Also considered were comments regarding Requirement R3 Part 3.3, the phrasing 'Like replacements', and defining the term. Rather than introduce a new definition, the SDT made modifications to shift the focus on "previously assessed configuration" as the reason why an active vulnerability assessment need not be reperformed. The intent is to require assessments to reduce the risk of introducing vulnerabilities to an existing environment when new Cyber Assets are being implemented, or when failures occur and existing Cyber Assets need to be replaced. The risk is associated with unassessed configurations for these Cyber Assets. A 1-for-1 replacement of an existing Cyber Asset with another, configured like the one being replaced, suggests the security posture is known as a function of the reconstruction process to build the replacement. Since the existing Cyber Asset had been previously assessed, the performance of the requirement part is not warranted. Entities can still choose to define the term ‘like replacements’ within their own programs and processes if the Registered Entity deems that necessary or a value add. The SDT removed the word "any" from the Measures for Requirement R3 Part 3.3 as requested. Regarding Requirement R4, Attachment 1, Section 1, Part 1.3 and the risk associated with the new bullet that reads, “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;”, the SDT agrees with the unintended consequence that this may leave a gap where newer software vulnerabilities could exist for an earlier known state that have not been addressed. The bullet was removed in response to this industry concern.

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro appreciates the opportunity to review and offers the following comments: 1. CIP-007 and CIP-005 Standards were modified to explicitly call out specific controls related to SCI (e.g. CIP-007 R1.3 / CIP-005 R1.3) but in CIP-010 R1 it is not written with the same clarity. For example, in CIP-010-3 R1.1 measures provided are not truly applicable to non SCI CIP-007 and CIP-005 controls. Operationally they differ greatly from non-SCI classified assets. Similar to the pattern followed in CIP-005 and CIP-007 changes, BC Hydro proposes to call out in a separate requirement SCI controls that need to be evaluated. 2. The inclusion of the following "... or intended changes to settings that could weaken configured cyber security controls required by CIP005 and CIP-007" makes the Requirement R1.1 of CIP-010-3 unclear. It is indicative that this Requirement will only apply if the change in settings has an effect on the configured CIP-007 and CIP-005 controls. However the expected scope of changes in settings need clear direction and guidance. Some pertinent use case examples and clear direction is needed here.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments. The SDT focused more on objective type language versus a prescriptive list and does not plan to separate virtualization requirements from the existing requirements at this time. The SDT considered your perspective, agreed it carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren believes that R1.1 is too large of a requirement and should be split up into multiple smaller requirements. In R2.1, Ameren would like examples of "settings that could weaken configured cyber security controls," because this could be left up to interpretation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT believes splitting R1.1 into multiple requirements could potentially create double jeopardy across requirements. However, the Part for verification of security controls was separated from Part 1.1 back into Part 1.4 to regain clarity on required actions that must occur as a part of the change authorized in Part 1.1. The SDT also considered your perspective the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed the language and refocused the requirement on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	No

Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	No
Document Name	
Comment	
Concerns regarding backward compatibility. And how compliance on existing practices will be assessed following the proposed change. Specifically how current practices related to “Live operating system and software executable only from read-only Media” can still need the intent of Section 1.3 without subjectivity inherent in the “other mitigation methods” option. Request adding of technical rationale (i.e. the intent of the change) for Attachment 1 Section 1.3. in particular explanation on the bullet that was added, i.e. “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution”. Support comment from NPCC RSC. Reiterated here: “For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT considered comments regarding Requirement R4, Attachment 1, Section 1, Part 1.3 and the risk associated with the new bullet that reads, “Controls that maintain the state of the operating system and software such that it is in a known state prior to	

execution;”. The SDT agrees with the unintended consequence that this may leave a gap where newer software vulnerabilities could exist for an earlier known state that have not been addressed. The bullet has been removed in response to this industry concern.

Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	No
Document Name	
Comment	

For requirement 1.1.2, we suggest to simply write, “Verify the required cyber security controls remain implemented”. There is confusion as to why “…as required as a part of the change” adds to the requirement.

However, the newest version is closer to what is done by industries. Old version address the case when a plan made its own programs in assembly language. Now, it’s more representative of the real world when third-party software executables are buy and install in systems.

1) It is unclear if Management Interface of Cyber System is in scope for CIP-010

Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document that their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls.

Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to software, or intended changes to settings . . .” Part 1.1 also says “Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .”

For Part 3,3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term. “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s.

For Part 3.3, request removing “any” from the first Measures bullet because any is a scope concern . . . where any is interpreted as “all.”

For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.

Likes 0	

Dislikes 0	
Response	

Thank you for your comment. Regarding Part 1.1.2, and the unintended implication that that entities must verify all “required cyber security controls remain implemented as required”, the SDT separated the requirement for verification of security controls from Part 1.1 back into Part 1.4 to regain clarity on required actions that must occur 'as a part of the change' authorized in Part 1.1, and scoped those verification actions to what was relevant to the changes so a complete compliance check for CIP-005 and CIP-007 is not required.

Yes, the Management Interface of a Cyber System is in scope for CIP-010. CIP-005 contains specific requirements for the controls that must be implemented for a Management Interface where the Glossary term is used within the Requirement or Requirement Part in CIP-005. A Management Interface is a component of a Cyber System, so where changes to the Management Interface's implemented cyber security controls serving the requirements in CIP-005 occur, those changes would be subject to CIP-010 requirements.

The SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The SDT agrees the use of "AND" vs "OR" in relation to the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."

Also considered were comments for Requirement R3 Part 3.3, the phrasing 'Like replacements', and defining the term. Rather than introduce a new definition, modifications were made to shift the focus on “previously assessed configuration” as the reason why an active vulnerability assessment need not be reperformed. The intent is to require active vulnerability assessments to reduce the risk of introducing vulnerabilities to an existing environment when new Cyber Assets are being implemented or when failures occur, and existing Cyber Assets need to be replaced. The risk is associated with unassessed configurations for these Cyber Assets. A 1-for-1 replacement of an existing Cyber Asset with another Cyber Asset that has been configured like the one being replaced suggests the security posture is known as a function of the reconstruction process to build the replacement, and because the existing Cyber Asset had been previously assessed, thereby not warranting the performance of the requirement part. Entities can still choose to define the term ‘like replacements’ within their own programs and processes if the Registered Entity deems that necessary or a value add. The word "any" was removed from the measure per your comment.

Regarding Requirement R4, Attachment 1, Section 1, Part 1.3 and the risk associated with the new bullet that reads “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;”, the SDT agrees this may leave a gap where newer software vulnerabilities could exist for an earlier known state that have not been addressed. This bullet was removed in response to this industry concern.

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No

Document Name	
Comment	
Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls. Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to software, or intended changes to settings . . .” Part 1.1 also says “Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .” For Part 3.3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term. “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s. For Part 3.3, request removing “any” from the first Measures bullet because any is a scope concern . . . where any is interpreted as “all.” For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Regarding the need for Measures to meet the Objectives and consistency of terms, and when modifying Requirement R1, the SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance, as well as to assure the virtualization components are also aligned. The TR was reviewed to ensure the baseline part is clear. The SDT made modifications to ensure consistent use of terms instead of the use of similar terms like “software patches” and “security patches” to further remove any concerns of unintended nuances from using synonymous terms interchangeably; cyber security patches is now the term used throughout. Also considered were comments for Requirement R3 Part 3.3, the phrasing 'Like replacements', and defining the term. Rather than introduce a new definition, modifications were made to shift the focus on "previously assessed configuration" as the reason why an active vulnerability assessment need not be reperformed. The intent is to require active vulnerability assessments to reduce the risk of introducing vulnerabilities to an existing environment when new Cyber Assets are being implemented or when failures occur, and existing Cyber Assets need to be replaced. The risk is	

associated with unassessed configurations for these Cyber Assets. A 1-for-1 replacement of an existing Cyber Asset with another Cyber Asset that has been configured like the one being replaced suggests the security posture is known as a function of the reconstruction process to build the replacement, and because the existing Cyber Asset had been previously assessed, thereby not warranting the performance of the requirement part. Entities can still choose to define the term ‘like replacements’ within their own programs and processes if the Registered Entity deems that necessary or a value add. The word "any" was removed from the Measures for Requirement R3 Part 3.3 as requested. Regarding Requirement R4, Attachment 1, Section 1, Part 1.3 and the risk associated with the new bullet that reads “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;”, the SDT agrees this may leave a gap where newer software vulnerabilities could exist for an earlier known state that have not been addressed. This bullet was removed in response to this industry concern.
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment
For requirement 1.1.2, we suggest to simply write, “Verify the required cyber security controls remain implemented”. There is confusion as to why “…as required as a part of the change” adds to the requirement. However, the newest version is closer to what is done by industries. Old version address the case when a plan made its own programs in assembly language. Now, it’s more representative of the real world when third-party software executables are buy and install in systems. {C}1) It is unclear if Management Interface of Cyber System is in scope for CIP-010 {C}2) The usage of ¨OR¨ seems to allow entities not to control changes to software. Suggest using the ¨AND¨ instead in ¨Control the implementation of intended changes to software, or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007¨ Request clarification of Part 1.1 since meeting the Measures may not meet the Objectives. Entity may need to document that their baselines (from previously approved Standard) when addressing their CIP-005 and CIP-007 security controls. Request consistent language in the Requirements of Parts 1.1 and 1.3. Part 1.1 provides what is included in software. Part 1.3 distinguishes some of 1.1 apart from software. Part 1.1 starts with “Control the implementation of intended changes to software, or intended changes to settings . . .” Part

1.1 also says “Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.” Part 1.3 starts with “Prior to the installation of operating systems, firmware, software, or software patches . . .”

For Part 3,3, request clarification on the first Requirement bullet – “Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System.” The term “like replacement” is an undefined term. Does the SDT intend for the entity to define this term. “Configuration of the previous” implies a baseline that was not specified. As written, the entity’s interpretation may be different than the auditor’s.

For Part 3.3, request removing “any” from the first Measures bullet because any is a scope concern . . . where any is interpreted as “all.”

For 1.3 in Attachment 1, recommend changing this new bullet from “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;” to “provide valid mitigation” since there may be newer software vulnerabilities that the earlier state has not addressed.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Regarding Part 1.1.2 and the unintended implication that that entities must verify all “required cyber security controls remain implemented as required”, the SDT separated the requirement for verification of security controls from Part 1.1 back into Part 1.4 to regain clarity on required actions that must occur 'as a part of the change' authorized in Part 1.1, and scoped Those verification actions to what was relevant to the changes so a complete compliance check for CIP-005 and CIP-007 is not required.

Yes, the Management Interface of a Cyber System is in scope for CIP-010. CIP-005 contains specific requirements for the controls that must be implemented for a Management Interface where the Glossary term is used within the Requirement or Requirement Part in CIP-005. A Management Interface is a component of a Cyber System, so where changes to the Management Interface's implemented cyber security controls serving the requirements in CIP-005 occur, those changes would be subject to CIP-010 requirements.

The SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance.

The SDT agrees the use of "AND" vs "OR" in relation to the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."

Also considered were comments for Requirement R3 Part 3.3, the phrasing 'Like replacements', and defining the term. Rather than introduce a new definition, modifications were made to shift the focus on "previously assessed configuration" as the reason why an active vulnerability assessment need not be reperformed. The intent is to require active vulnerability assessments to reduce the risk of introducing vulnerabilities to an existing environment when new Cyber Assets are being implemented or when failures occur, and existing Cyber Assets need to be replaced. The risk is associated with unassessed configurations for these Cyber Assets. A 1-for-1 replacement of an existing Cyber Asset with another Cyber Asset that has been configured like the one being replaced suggests the security posture is known as a function of the reconstruction process to build the replacement, and because the existing Cyber Asset had been previously assessed, thereby not warranting the performance of the requirement part. Entities can still choose to define the term ‘like replacements’ within their own programs and processes if the Registered Entity deems that necessary or a value add.

Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

In the proposed language, the term “could weaken” as it applies to changes requiring configuration management controls is vague and, as undefined, leaves the determination unsupported by existing definitions. GSOC suggests either substituting “alters” or adding “ . . . as determined by the responsible entity”. As proposed, change management controls would only need to be utilized for a type of change that undermines existing security and not for all changes.

Additionally, as proposed, the language of 1.1.2 could subject the responsible entity to double jeopardy violationof CIP-010 as well as the underlying violations of CIP-005 and CIP-007.. Additionally, as written, every control must be reviewed for every applicable change regardless of whether it is technical, procedural, or impacted by the change. GSOC recommends the removal of 1.1.2 as a separate requirement and inclusion in measures.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused the Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.".

Regarding Part 1.1.2 and the unintended implication that that entities must verify all “required cyber security controls remain implemented as required”, the SDT separated the requirement for verification of security controls from Part 1.1 back into Part 1.4 to regain clarity on required actions that must occur as a part of the change authorized in Part 1.1, and scoped those verification actions to what was relevant to the changes so a complete compliance check of CIP-005 and CIP-007 is not required.	
JT Kuehne - AEP - 6	
Answer	No
Document Name	
Comment	
AEP appreciates SDT’’s efforts in making requirements more clear. However, AEP does not support R1.2 and R2.1 and states recommendations below. • **R 1.2.1**: SDT added **“the configuration of”** as in “…where the test is performed in a manner that minimizes adverse effects to ensure **that the configuration of** required cyber security controls in CIP-005 and CIP-007 reamin implemented as required”. AEP suggests removing this added language as it is too prescriptive. • **R2.1**: AEP questions the statement "*unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007*" and recommend SDT to revert the requirement languages as proposed in Draft #3, i.e., “Methods to monitor for unauthorized changes at least once every 35 calendar days. Document and investigate detected unauthorized changes.”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees with your comments about the prescriptive nature of the language "the configuration of" in proposed Part 1.2.2 and removed that language. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R2 Part2.1. The SDT removed this language and refocused Requirement R2 Part 2.1 on methods to monitor for "...unauthorized changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement part CIP-007, as defined by the Responsible Entity."	
Kimberly Turco - Constellation - 6	
Answer	No
Document Name	

Comment	
Constellation supports comments that were submitted by Exelon Corporation. Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See response to Exelon Corporation.	
Alison Mackellar - Constellation - 5	
Answer	No
Document Name	
Comment	
Constellation supports comments that were submitted by Exelon Corporation. Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDTs response to Exelon Corporation.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	No
Document Name	
Comment	
ITC supports the comments written in the EEI response	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the SDTs response to EEI.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
R1-Removing baseline configuration does not change what needs to be done in practice. Entities will still need to retain a baseline configuration as evidence from which to establish the changes that were authorized. · For Part 1.1 an entity will still need to show the baseline configuration prior to the change to show required cyber security controls in CIP-005 and CIP-007 are not adversely affected. · For Part 2.1 an entity will still need to provide baseline configurations for evidence that they monitor at least once every 35 calendar days for unauthorized changes to the items listed Parts 1.1 and 1.2. For R3-the concern is that Remediation VLANs should be properly defined in the technical rational or Glossary as it may introduce situations where an entity could inadvertently place production Cyber Assets in this VLAN.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees entities will need a means to demonstrate changes that alter the behavior of one or more cyber security controls serving one or more requirement parts in CIP-005 or CIP-007 were authorized in accordance with Requirement R1 Part 1.1, and maintaining a baseline is one method an entity can choose to demonstrate their practices. The SDT considered your comments regarding Remediation VLANs and reviewed TR related to this functionality. The SDT did not create a new Glossary of Terms definition.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	

Answer	No
Document Name	
Comment	
In large part, the proposed changes are fine. However, there is an implication by virtue of the new veribiage and removal of “baseline configurations” that additional configuration items (outside of the original “baseline configuration”) need to be included within change management. Such additional configuration items are not explicitly included in the Measures section, thus leaving this aspect of the requirement wholly subjective. Additionally, the third bullet on slide 39 from the Project 2016-02 Webinar seems to implicitly add a documentation requirement for the analysis/comparison of baseline configurations to security controls. This ask is not in the requirement. Including it in the Webinar presentation empowers Regional auditors to ask for evidence of requirements that are not included in the standard or measures sections.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT considered the suggestion to reintroduce the word 'baseline' so R1 would provide clarity on 'how' to meet the requirement using a 'baseline'. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. Additionally, the SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to add clarity that an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", and which changes then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way how an entity can choose to demonstrate compliance. The SDT reviewed TR based on comments provided to ensure the baseline part is clear and understood. Lastly, the SDT agrees Requirement R1 does NOT include a documentation requirement for the analysis/comparison of baseline configurations to security controls.	
Kristine Martz - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	

AWS agrees with changes to CIP-010 R1, R2, and R3. However, AWS remains concerned that CIP-010 R4 does not address security risks associated with virtual machines (VM) hosted on physical Transient Cyber Assets (TCAs) because the standard language states that a VM running on a physical TCA can be treated as software. We acknowledge the SDT response to the previous comments in the consideration of comments, but we still see security risks and have provided our previous comment below for context.

The Standard allows an entity to choose one or a combination of security controls that may not extend cyber security protections to the VM itself leaving VMs potentially vulnerable to security threats undetected by the physical host. We propose removing the language “Virtual machines hosted on a physical TCA can be treated as software on that physical TCA” from the TCA definition. By removing this language, entities would be required to apply security controls to the virtual machines hosted on their physical TCAs in alignment with CIP-010 R4.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT considered your concerns and concluded that a VM on a TCA would be considered software on the TCA and subject to Requirement R4, Attachment 1 from that perspective. Additional information can be found in the TR.

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	

Comment

The current phrasing of Part 1.1.2 implies that entities must verify all “required cyber security controls remain implemented as required” for any change to software or security settings even if the change itself does not impact a certain control (e.g. a windows patch typically doesn’t modify an ESP/EAP for CIP-005, updating a FW Policy does not impact CIP-007 R2, etc.). This new language removes entities abilities to identify potential impacts and verify/test those impacts as allowed by the in-effect standard and the previous revision. Entergy is concerned that this language as written would require entities an undue burden to re-verify non-impacted controls for every change. While the Measures section implies that an entity has latitude to identify which cyber security controls should be verified (“ a list of cyber security controls verified”) this is not clearly aligned with the language of the standard.

Entergy recommends adding clarifying language to CIP-010 R1 Part 1.1 that entities verify potentially impacted cyber security controls, such as “Verify the required cyber security controls ***identified by the Responsible Entity that could be weakened*** remain implemented as required as part of the

change.” This would allow entities to focus verification efforts on potentially impacted controls based on the nature of the change, instead of a one-size fits all approach of re-verifying every CIP-005 and CIP-007 control for every change.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Regarding Part 1.1.2 and the unintended implication that that entities must verify all “required cyber security controls remain implemented as required”, the SDT separated the requirement for verification of security controls from Part 1.1 back into Part 1.4 to regain clarity on required actions that must occur as a part of the change authorized in Part 1.1 and scoped those verification actions to what was relevant to the changes so a complete compliance check of CIP-005 and CIP-007 is not required. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	No
Document Name	
Comment	
In large part, the proposed changes are fine. However, there is an implication by virtue of the new veribiage and removal of “baseline configurations” that additional configuration items (outside of the original “baseline configuration”) need to be included within change management. Such additional configuration items are not explicitly included in the Measures section, thus leaving this aspect of the requirement wholly subjective. Additionally, the third bullet on slide 39 from the Project 2016-02 Webinar seems to implicitly add a documentation requirement for the analysis/comparison of baseline configurations to security controls. This ask is not in the requirement. Including it in the Webinar presentation empowers Regional auditors to ask for evidence of requirements that are not included in the standard or measures sections.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. Additionally, the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to add clarity that an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", and which changes then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way how an entity can choose to demonstrate compliance. The SDT reviewed TR to ensure the baseline part is clear.

Lastly, Requirement R1 does NOT include a documentation requirement for the analysis/comparison of baseline configurations to security controls.

Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County

Answer	No
Document Name	

Comment

CIP-010 R2.1 as written would require an audit of every setting that could impact a CIP-005 or CIP-007 security control every 35 calendar days on High Impact devices. For some devices, this could be hundreds of individual settings, and Cyber Assets may not provide these settings in a way that audit of those settings could be automated. This would also effectively be a baseline configuration, though a more rigorous one than required by the currently effective requirements, as each setting would have a “baseline” to ensure the effectiveness of the security control it implements.

Chelan finds it difficult to develop a requirement that accomplishes the same security objective CIP-010 R2.1 of auditing that unauthorized changes have not occurred without the development of a baseline configuration to compare against. By definition, auditing changes requires you to have a known good state, essentially a baseline configuration. If the SDT wishes to eliminate baseline configurations, it should eliminate the periodic monitoring for unauthorized changes, or change the security objective.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT agrees there is potential for confusion, or perceived scope increase or misinterpretation by use of terms like "settings" would be interpreted as too prescriptive, so this phrasing was removed.

After careful consideration, the SDT chose not to reintroduce the word 'baseline', and chose to keep the monitoring component in Requirement R2 by providing greater clarity on the scope and objectives of each requirement. The prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement with 'baselines' as one means to achieve the objective. The focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to add clarity that an entity can choose to continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007..." require authorization per Requirement R1 Part 1.1. Changes to high impact BES Cyber Systems and their associated 1. EACMS; and 2. PCA, and SCI supporting an Applicable System in Requirement R2 Part 2.1 are then subject to the monitoring requirements in Requirement R2 Part 2.1. The SDT focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear. Additionally, The SDT refocused Requirement R2 Part 2.1 on methods to monitor for "...unauthorized changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement part CIP-007, as defined by the Responsible Entity." to further ensure this requirement is not misinterpreted as a mini audit of CIP-005 and CIP-007.

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	No
Document Name	

Comment

Similar to the MRO-NSRFs response, WEC Energy Group wishes to bring attention to the added phrase in CIP-010 Requirement 1 Part R1.1, "…or intended changes to settings that could weaken configured cyber security controls required by CIP005 and CIP-007." We also would raise concerns with the current proposed Measures for R1.1.

This language raises questions. On applicable systems, are entities expected to authorize/monitor for both software changes AND settings that could weaken cyber security controls. Or does the 'or' indicate that choosing one of those would fulfill the obligations? For instance, consider a password change on a service account/agent which unintentionally breaks logging capabilities on an unspecified BCA. While an entity would be in violation of CIP-007 R4, with this new CIP-010 language, would the password change constitute a "change to settings" which weakened a CIP-007 control (R4.2) and therefore have been required to navigate the change management process? Would simply changing an applicable password from 10 characters to 9 characters constitute a weakening of CIP-005/CIP-007 cyber security controls?

There are many configuration changes that currently don't affect one of the baseline items but could be considered in scope in the new version of the standard (for example, modification of anti-virus settings or any configuration settings on a firewall). This addition, combined with one of the statements made during the September 12, 2022 webinar that entities may have more compliance work to perform under the revised CIP-010, indicates that the scope of change management is broadened under the proposed revisions. This directly contradicts other statements that have

stressed how the revisions are to be backwards compatible. The idea being that any entity that is in compliance today with current technologies and processes will be compliant under the revised standards, even if they do not seek to employ or utilize virtualization technologies. We recommend the SDT to revisit the proposed CIP-010 R1.1 language and undertake any further revision needed to ensure that the scope of CIP-010 R1 is not expanded any more than necessary. One recommendation would be to separate both R1.1 into two parts, one addressing BCAs only, which would mirror existing CIP-010-3 R1.1 language, and one addressing SCI specifically which would further clarify “settings” (this would also necessitate splitting the proposed R2.1 into two different requirements as well). Secondly, it seems that there continues to be confusion in the industry over whether or not to baseline and what are the best methods by which to demonstrate compliance with CIP-010 R1.1. We note that, while the Measures for R1.1 are quite lengthy, all the detail is about what the “documented process” should address or include, without suggesting examples of what the documented process could actually be documented as. We approve of providing options for entities to comply with CIP-010 R1.1 without necessarily having to maintain and demonstrate a documented baseline but it’s also true that many utilities wish to continue using precisely that approach for their compliance – yet the word baseline is missing entirely from the Measures section of CIP-010 R1.1. We understand that “documented process” that includes the various items listed implies a baseline, but there is no reason we see not to just then come out and say “baseline” is an example of an acceptable option.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Also see response to MRO NSRF. The SDT agrees the on terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused the Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity." Regarding the potential for confusion, perceived scope increase or misinterpretation by the use of terms like "settings" would be interpreted as too prescriptive, so this phrasing was removed. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. Additionally, the SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to add clarity that an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", then require authorization per Requirement R1 Part 1.1.	

The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	No
Document Name	
Comment	
The new proposed wording is challenging to navigate and subjective. For example, what does it mean to weaken the configured cybersecurity controls and settings? We recommend changing CIP-010 R1.1 back to the previous wording, and restore previous requirement parts through R2.1, and add “SCI supporting an Applicable System in this Part”. This change is out of scope to support virtualization other than adding SCI to the applicability column. The proposed changes do nothing to support virtualization but do add significant ambiguity to the requirement. Also, a baseline MUST be established if there is going to be a requirement to monitor for unauthorized changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.". The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. The SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to add clarity that an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007..." then require authorization per Requirement	

R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed to ensure the baseline part is clear.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

The MRO NSRF wish to bring attention to the added phrase in CIP-010 Requirement 1 Part R1.1, "…or intended changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007." The MRO NSRF also would raise concerns with the current proposed Measures for R1.1.
This language raises questions. On applicable systems, are entities expected to authorize/monitor for both software changes AND settings that could weaken cyber security controls. or does the 'or' indicate that choosing one of those would fulfill the obligations? For instance, consider a password change on a service account/agent which unintentionally breaks logging capabilities on an unspecified BCA. While an entity would be in violation of CIP-007 R4, with this new CIP-010 language, would the password change constitute a "change to settings" which weakened a CIP-007 control (R4.2) and therefore have been required to navigate the change management process? Would simply changing an applicable password from 10 characters to 9 characters constitute a weakening of CIP-005/CIP-007 cyber security controls?
There are many configuration changes that currently don't affect one of the baseline items but could be considered in scope in the new version of the standard (for example, modification of anti-virus settings or any configuration settings on a firewall). This addition, combined with one of the statements made during the September 12, 2022 webinar that entities may have more compliance work to perform under the revised CIP-010, indicates that the scope of change management is broadened under the proposed revisions. This flies in the face of other statements that have stressed how the revisions are to be backwards compatible and that any entity that is in compliance today with current technologies and processes will be compliant under the revised standards even if they do not seek to employ or utilize virtualization technologies.

Secondly, it seems that there continues to be confusion in the industry over whether or not to baseline and what are the best methods by which to demonstrate compliance with CIP-010 R1.1. The MRO NSRF note that, while the Measures for R1.1 are quite lengthy, all the detail is about what the "documented process" should address or include, without suggesting examples of what the documented process could actually be documented as. The MRO NSRF approve of providing options for entities to comply with CIP-010 R1.1 without necessarily having to maintain and demonstrate a documented baseline but it's also true that many utilities wish to continue using precisely that approach for their compliance – yet the word baseline is missing entirely from the Measures section of CIP-010 R1.1. The MRO NSRF understand that "documented process" that includes the various items listed implies a baseline, but there is no reason the MRO NSRF see not to just then come out and say "baseline" is an example of an acceptable option.

The MRO NSRF recommend that the first paragraph of R1.1 Requirement be rewritten to read, "Control the implementation of intended changes to Applicable Systems that could weaken configured cyber security controls required by CIP-005 and CIP-007." The MRO NSRF also recommend the inclusion of the word "baseline" as an example in the R1.1 Measures of a type of documented process that Registered Entities may employ to

demonstrate their compliance with R1.1. Alternatively, if this recommendation is not acceptable, then some other change in verbiage that provides Entities the option of either continuing to comply using current baseline and baseline deviation tracking methods, or allowing a different approach per the new requirement and measure language, to ensure for the allowance of backward compatibility.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity." Regarding the same terminology for Requirement R2 Part 2.1, the SDT refocused Requirement R2.1 on methods to monitor for "...unauthorized changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement part CIP-007, as defined by the Responsible Entity." The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. The SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to confirm an entity can continue using baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance.	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
In Measures to revised R1.1.2, the only example given of a tool used to verify required security controls [required by CIP-005 and CIP-007] remain implemented is a vulnerability scanner. It is unlikely that this will be the tool used to verify these controls, and that guidance may be misleading to Regional Entity auditors. It is more likely that a configuration management database will be used to verify that software is installed and that controls	

such as listening ports, disabled accounts, password controls, antimalware settings, and applied security patches are unchanged. CEHE recommends that the SDT add "configuration management database" as an example in the Measures in R1.1.2.

In R3.3, the exception for replacement of the same type of Cyber System with a configuration of the previous or other existing Cyber System should be revised to include additions of the same type, not only replacements. An example is adding a console from an identical known good image as existing consoles. This is not a replacement, but from a security and reliability perspective, has the same effect. Language should be revised to say "Like replacements or additions of the same type of Cyber System with a configuration of the previous or other existing Cyber System".

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT chose to split Requirement R1 Part 1.1.2 back out into Part 1.4 and made modifications to enable virtualization. The measures were rewritten to align with the reinstated Part 1.4.

The SDT agrees and made modifications to shift the focus on "previously assessed configuration" as the reason why an active vulnerability assessment need not be reperformed.

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	No
Document Name	

Comment

In Measures to revised R1.1.2, the only example given of a tool used to verify required security controls [required by CIP-005 and CIP-007] remain implemented is a vulnerability scanner. It is unlikely that this will be the tool used to verify these controls, and that guidance may be misleading to Regional Entity auditors. It is more likely that a configuration management database will be used to verify that software is installed and that controls such as listening ports, disabled accounts, password controls, antimalware settings, and applied security patches are unchanged. SIGE recommends that the SDT add "configuration management database" as an example in the Measures in R1.1.2.

In R3.3, the exception for replacement of the same type of Cyber System with a configuration of the previous or other existing Cyber System should be revised to include additions of the same type, not only replacements. An example is adding a console from an identical known good image as existing consoles. This is not a replacement, but from a security and reliability perspective, has the same effect. Language should be revised to say "Like replacements or additions of the same type of Cyber System with a configuration of the previous or other existing Cyber System".

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
For R2 Dominion Energy recommends reverting back to the previous language and include verbiage excluding password changes. The term “settings” is too subjective and can be interpreted inconsistently. Additionally, for the Severity Level for R1, Dominion believes the SAR was intended to address virtualization and arbitrarily changing the VSL for R1 is not in scope. Dominion recommends reverting back to the previous language	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the use of terms like “settings” have the potential for confusion, perceived scope increase or misinterpretation would be interpreted as too prescriptive, so this phrasing was removed. The SDT revisited comments regarding VSLs and SAR in preparation for the next draft.	
Israel Perez - Salt River Project - 6	
Answer	No
Document Name	
Comment	
We still have concerns on CIP-010-5 because the draft does not include the Guidelines and Technical Basis section where it defines what must be included in a vulnerability assessment. It is understood that the Standards Drafting team emphasizes backwards compatibility, but, the proposed	

changes to CIP-007 R1 and CIP-010 R1.1 could affect what is required in the vulnerability assessments. At the very least, we would like to know and comment on what additional items will be required for SCI in a vulnerability assessment as there is nothing found in the current proposed changes. Lastly, under CIP-010 R3.3 BES Cyber System is shortened to BCS. However, this is different than the other parts of CIP-010 R3. We recommend consistency.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The reinstatement of Guidelines and Technical Basis (GTB) is out of scope for the project 2016-02 SAR. The Technical Rationale Transition Plan to revise the Reliability Standards template to eliminate the GTB section and allow for the creation of a separate document containing the TR was endorsed by the NERC Standards Committee on January 17, 2018. The use of the term “guideline” in GTB has created confusion for some stakeholders on the use of information in this section for guidance in developing compliance approaches, and the TR for Reliability Standards team was formed to clarify the intended use of information in this section, and to address that confusion. The purpose of this project was to further clarify the principles, development, and use of GTB (historically) and TR. The ERO continues to assess compliance based on the language of the Reliability Standard and the facts and circumstances presented. With the enactment of the Compliance Guidance Policy, it appears helpful to further clarify the distinction between Implementation Guidance and GTB (or TR, as explained below). GTB should focus on TR that assists technical understanding of a requirement and/or Reliability Standard. GTB should not include compliance examples or compliance language. Such information, if needed, should be developed as Implementation Guidance under the Compliance Guidance Policy. As a result, the SDT established a separate TR document. Any Implementation Guidance proposed by the SDT must go through the ERO endorsement process. Additionally, the SDT took another pass through the draft to assure consistency with the use of the acronym BCS for BES Cyber System throughout.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes modifications to CIP-010 should be limited to conforming changes only.	
Likes 0	
Dislikes 0	

Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern disagrees with Part 1.1 Requirements that includes the phrase “settings that could weaken cyber security controls required by CIP-005 and CIP-007”. Southern finds this phrase overly broad, questioning if full compliance could ever be proven out of the universe of “settings” (registry settings, configuration paramenters, per application settings, etc.). Added to the complexity of knowing all settings is the phrase “could weaken” adding in the idea of ‘potential’ to this already elusive scope. Southern suggests the SDT reconsider the concept used in draft 3 of the entity defining the higher level types of changes they have in their change management programs. In addition, to provide further clarity of scope, Southern suggests the SDT go through CIP-005 and CIP-007 and list the areas that should be under CIP-010 change management. Since these requirements are the same for every entity, that list should be the same for every entity.	
Likes 0	
Dislikes 0	
Response	
The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity."	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
The language “…changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007” is subjective. There could be any number of “settings” that “could weaken” the security controls. Can guidance be given such as some exapmples of these settings that could be	

used to weaken the security controls? Also, is “software patches” synonymous with “security patches” or are these two (2) different entities of their own?	
Likes 0	
Dislikes 0	
Response	
The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity." Additionally, modifications were made to remove concerns of unintended nuances from using synonymous terms interchangeably. Cyber security patches is now the term used throughout.	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
We feel using “could” in parts of CIP-010-5 is very subjective and is not necessary. Further the measures uses “may” instead of “could”. A change either does or doesn’t affect cybersecurity controls required by CIP-005 and CIP-007. We are fine with the language, but feel it would be cleaner and less ambiguous without “could”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the requirement language must be clear and unambiguous as to ‘what’ is required and removed the word "could". The SDT chose to keep the word "may" within the Measures because the data in this column is intended to provide examples of possible ways an entity can demonstrate compliance, but it is not the only way nor is it a requirement. The flexibility of 'how' through the use of "may" in the Measures is appropriate.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes

Document Name	
Comment	
EEI supports the revisions made to CIP-010 for Draft 4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
NEE requests the SDT apply linkages in CIP-010-5 R1 P1.1 to all subparts for software scope. Suggest clarity that all subparts refer back to the software scope definition established in CIP-010-5 R1 P1.1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT modified the Parts that hinge on the scoping in Part 1.1. by adding "change from Part 1.1" to provide clear linkage and scoping.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments that were submitted by the MRO NERC Standards Review Forum.	

Likes 0	
Dislikes 0	
Response	

Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
Document Name	

Comment

PG&E supports the modification made to CIP-010, but PG&E provides the following recommendation:

The text of "…intended changes to settings ..." withing the Requirement language be clarified to avoid un-intended consequence of setting changes that would not have an impact on the CIP-005 and CIP-007 controls from being brought into scope of Audit Teams.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT agrees the potential for confusion, perceived scope increase or misinterpretation by use of terms like "settings" would be interpreted as too prescriptive, so this phrasing was removed.

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

NV Energy supports the revisions for CIP-010-5, but harbors some concern regarding unclear language in Requirement R1, subpart 1.1. The word "settings" does not enjoy the same clarifying language as does the word "software". We believe this creates a risk for unpredicatble interpretation without any additional technical rationale defining the intent of the word. NV Energy suggests "settings" receive a definition complementary to "software" to better assist entities reach compliance, but ultimately feels the language in its current state is workable although not ideal.

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the potential for confusion, perceived scope increase or misinterpretation by use of terms like "settings" would be interpreted as too prescriptive, so this phrasing was removed.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed changes to CIP-010 but feel the following "weaken" statement introduced in part R1.1, without an official definition, leads to uncertainty and lack of clarity around the items that may fall into change management. This will result in re-examination of existing systems and baselining methodologies that threaten the intended backwards compatibility of the new requirements. In addition, we agree with EEI stance that which “settings” are in scope requires additional clarification.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT agrees the terminology "could weaken" carried unintended consequences and did not appropriately scope Requirement R1. The SDT removed this language and refocused Requirement R1 Part 1.1 on authorization for "...changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity." Also see response to EEI regarding comments on the term "settings".	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

BPA believes CIP-010 R2.1 needs a verb in front of beginning of the Requirement language.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. See parent Requirement R2 for the verb, as the action is "to implement".	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	

Likes 0

Dislikes 0

Response

See response to EEI.

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE continues to be concerned security obligations will be reduced by removing an explicit requirement for Registered Entities to create and maintain baseline configuration documentation.

Establishing and maintaining baseline configurations represent best practices for system hardening. Texas RE recommends adhering to NIST Special Publication 800-53 (Rev. 5), CM-2 Baseline Configuration, which states, “Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.”

NIST Special Publication 800-53 (Rev. 5) provides additional information, such as using tools to track version numbers on operating systems, applications, types of software installed, and current patch levels in order to maintain the currency, completeness, accuracy, and availability of the baseline configurations of systems. This is information that is currently captured within existing baseline documentation requirements.

If the drafting team has concerns that maintaining baseline documentation of dynamic VMs is not technically feasible, Texas RE suggests adding the verbiage “per system capability” to CIP-010 R1’s baseline requirements. Registered Entities have demonstrated that the vast majority of systems, both physical and virtual, are capable of having baseline documentation created, tracked, and updated as necessary. As such, this requirement should remain in place for those systems where it is technically feasible to perform this industry best security practice.

Likes 0

Dislikes 0

Response

Thank you for your comments. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. The SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement. To maintain backwards compatibility, the SDT introduced the terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. to confirm an entity can continue using baselines as the method to determine which changes "...alter the

behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", then require authorization per Requirement R1 Part 1.1. The SDT also focused on aligning the Measures by mapping the updated concept to the former 'baseline' attributes to further demonstrate 'baselines' remain one way an entity can choose to demonstrate compliance. The TR was reviewed TR to ensure the baseline part is clear.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying CIP-010 to allow for more flexibility in tracking changes to applicable systems while maintaining and even increasing security.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	

7. The SDT revised CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 mostly with conforming changes or scoping clarifications related to SCI. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

As mentioned earlier, disagree with adding R1.6 to CIP-005 as CIP-005 is written for protections of logical devices and data. This should be restored back to CIP-006 R1 Part 1.10.f7.

Likes 0	
Dislikes 0	

Response

Thank you for your response. The SDT feels that R1.6 consolidates requirements together and removes the possibility for double jeopardy.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST disagrees with proposed changes to CIP-003 and CIP-011 due to the fact proposed changes go beyond conforming changes.

NST disagrees with proposed changes to CIP-009, as omitting SCI from all Requirements and Parts except for R1 Part 1.5 it would establish “implied requirements,” as discussed in our comments on Question 9, below. NST acknowledges that in some recovery situations, it might only be necessary to recover a virtual BES Cyber System and not its supporting SCI. However, given that failure or destruction of an SCI could, in some scenarios, wipe out an entire Control Center, NST believes that inclusion of SCI in a Responsible Entity’s recovery plan(s) should be mandatory rather than a suggested best practice.

NST agrees with proposed conforming changes to CIP-004, CIP-006, CIP-008 and CIP-013.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. CIP-009's focus is to ensure that the BCS can be recovered. An Entity can choose to recover that functionality of the BVCS in any manner that restores that functionality, potentially without the use of SCI, even if the original BCS included the use of SCI. Additionally, the majority of organizations making use of virtualization today will choose the All-In model where the underlay is classed as a part of the BCS itself. In this instance the underlay (not technically SCI) would be subject to the recovery requirements.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Since the Glossary modifications are the foundation to all Standard changes, NERC should seek approval of the new terms prior to any changes being introduced in the Standards to reduce potential misunderstanding or misinterpretation of both the new definitions and modified Standards. This will also allow NERC, and industry, time to determine additional courses of action, reduce confusion, and reduce additional risk associated with such wholesale changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT disagrees as many will not vote to approve terms (particularly technology terms) and definitions in a vacuum with no context as to how those definitions will be used. At times terms are created to match the requirements, such as IRA. Many may say that the IRA definition is too restrictive. However it is defined so that it matches scenarios where the CIP-005 R2 requirements can be met without affecting functionality or reliability of systems.	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	

Comment	
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;" Request clarification on execution of what? Perhaps "execution" should be changed to "entity use" For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC For CIP-006, Part 1.3 consider changing from "per system capability" because "per system capability" is an inadvertent get-out-of-jail. For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2 For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with "all" in the new language. The new Part 1.2.5 says " Verification of software integrity and authenticity of all software and patches provided by the vendor . . ." The R1 applicable systems language is "for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI)." We suggest that the scope should be "applicable systems," not all software and patches by the vendor.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been changed to include SCI as a conforming change. CIP-003 Attachment 1 references to the bullet that started with "Controls that maintain the state of the operating system and software such that..." have been removed. This option did not perform the security objective that it was designed to fulfill. The SDT chose to modify the Applicable Systems found in CIP-004 R2 through R6 to include references to Medium impact BCS with IRA in order to align the CIP-004 requirements with the new definition of IRA which includes electronic access without ERC.	

The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity to prove that the system is not capable as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable. The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves. The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section’s scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says “Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;” Request clarification on execution of what? Perhaps “execution” should be changed to “entity use” For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC For CIP-006, Part 1.3 consider changing from “per system capability” because “per system capability” is an inadvertent get-out-of-jail. For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2 For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with “all” in the new language. The new Part 1.2.5 says “ Verification of software integrity and authenticity of all software and patches provided by the vendor . . .” The R1 applicable systems language is “for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI).” We suggest that the scope should be “applicable systems,” not all software and patches by the vendor.	

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been changed to include SCI as a conforming change.

CIP-003 Attachment 1 references to the bullet that started with “Controls that maintain the state of the operating system and software such that..." have been removed. This option did not perform the security objective that it was designed to fulfill.

The SDT chose to modify the Applicable Systems found in CIP-004 R2 through R6 to include references to Medium impact BCS with IRA in order to align the CIP-004 requirements with the new definition of IRA which includes electronic access without ERC.

The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity to prove that the system is not capable as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable.

The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves.

The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.

Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC

Answer	No
Document Name	

Comment

For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section’s scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident

For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says “Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;” Request clarification on execution of what? Perhaps “execution” should be changed to “entity use”

For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC

For CIP-006, Part 1.3 consider changing from “per system capability” because “per system capability” is an inadvertent get-out-of-jail.

For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2

For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with “all” in the new language. The new Part 1.2.5 says “ Verification of software integrity and authenticity of all software and patches provided by the vendor . . .” The R1 applicable systems language is “for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI).” We suggest that the scope should be “applicable systems,” not all software and patches by the vendor.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been changed to include SCI as a conforming change.

CIP-003 Attachment 1 references to the bullet that started with “Controls that maintain the state of the operating system and software such that..." have been removed. This option did not perform the security objective that it was designed to fulfill.

The SDT chose to modify the Applicable Systems found in CIP-004 R2 through R6 to include references to Medium impact BCS with IRA in order to align the CIP-004 requirements with the new definition of IRA which includes electronic access without ERC.

The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity to prove that the system is not capable as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable.

The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves.

The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.

Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo

Answer	No
Document Name	

Comment

Same comment as for CIP-010, Q6.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Please see the response to Q6.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee

Answer	No
Document Name	

Comment

For CIP-003, Attachment 1, Section 4, request confirmation that while this Section has no updates, this Section's scope is bigger because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident

For CIP-003, Attachment 1, 5.1, requests clarification of the new bullet which says "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;" Request clarification on the execution of what? Perhaps "execution" should be changed to "entity use"

For CIP-004, R5 requests confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents . . . due to the updated definitions of IRA and ERC

For CIP-006, Part 1.3 consider changing from "per system capability" because "per system capability" is an inadvertent get-out-of-jail.

For CIP-011, request clarification on the double jeopardy between R2 and Part 1.2

For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with "all" in the new language. The new Part 1.2.5 says " Verification of software integrity and authenticity of all software and patches provided by the

vendor . . .” The R1 applicable systems language is “for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI).” We suggest that the scope should be “applicable systems,” not all software and patches by the vendor.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been changed to include SCI as a conforming change. CIP-003 Attachment 1 references to the bullet that started with “Controls that maintain the state of the operating system and software such that..." have been removed. This option did not perform the security objective that it was designed to fulfill. The SDT chose to modify the Applicable Systems found in CIP-004 R2 through R6 to include references to Medium impact BCS with IRA in order to align the CIP-004 requirements with the new definition of IRA which includes electronic access without ERC. The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity to prove that the system is not capable, as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable. The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves. The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	

For CIP-003, Attachment 1, Section 4, request confirmation that, while this Section has no updates, this Section's scope is being expanded because of changes to the definitions of Cyber Security Incident and Reportable Cyber Security Incident .

For CIP-003, Attachment 1, 5.1, request clarification of the new bullet which says "Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;" The language should be clarified to explain the word "execution" (i.e., on execution of what?) Perhaps "execution" should be changed to "entity use".

For CIP-004, R5 request confirmation that entities should re-evaluate serial connections because they may now be in scope for incidents due to the updated definitions of IRA and ERC.

For CIP-006, Part 1.3 consider changing from "per system capability" because "per system capability" is an inadvertent "get-out-of-jail free card.

For CIP-011, the double jeopardy between R2 and Part 1.2 should be clarified.

For CIP-013, Part 1.2.5 consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. The use of the word "all" in the new language is of concern. The new Part 1.2.5 says " Verification of software integrity and authenticity of all software and patches provided by the vendor . . ." The R1 applicable systems language is "for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI)." The scope should be "applicable systems," not all software and patches by the vendor.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The scope of CIP-003 Requirement 2 applies to all Sections of Attachment 1, so the scope has been changed to include SCI as a conforming change.

CIP-003 Attachment 1 references to the bullet that started with "Controls that maintain the state of the operating system and software such that..." have been removed. This option did not perform the security objective that it was designed to fulfill.

The SDT chose to modify the Applicable Systems found in CIP-004 R2 through R6 to include references to Medium impact BCS with IRA in order to align the CIP-004 requirements with the new definition of IRA which includes electronic access without ERC.

The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity to prove that the system is not capable, as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable.

The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves.

The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

No: Application Containers need to be defined with additional clarity.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. See the CIP Definitions and Exemptions Technical Rationale document posted with Draft 5 for additional clarification on the reasoning behind treatment of application containers as software of a VCA or CA.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)

Answer	No
Document Name	

Comment

For CIP-006, Part 1.3, consider changing from "per system capability" to "if technically feasible" because "per system capability" is an inadvertent get-out-of-jail.

For CIP-011, the SRC requests clarification on the double jeopardy between R2 and Part 1.2. Both sections apply to the handling and use of BCSI. If you violate R2, you will have mishandled or misused R1.2.

*For CIP-013, Part 1.2.5, consider including the mention of the applicable systems referenced in R1. This update avoids audit scope creep. Concerned with "all" in the new language. The new Part 1.2.5 says " Verification of software integrity and authenticity of all software and patches provided by the vendor . . ." The R1 applicable systems language is "for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI)." We suggest that the scope should be "applicable systems," not **"all"** software and patches by the vendor.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT chose not to modify the "per system capability" statement in CIP-006 R1 Part 1.3. The burden is now to document that the system is truly not capable, and if so, the Entity is not forced to perform the requirement. However, it does not offer a get-out-of-jail option. The burden is on the entity to prove that the system is not capable, as a system. If a component can be replaced within the system in order to perform the required function, then the system is capable. The SDT asserts that CIP-011 R1.2 & R2.1 represent different control sets on different targets. R1 targets the BCSI associated with the Applicable Systems, and R2 targets the Applicable Systems themselves. The SDT included a reference to the applicable systems from R1 within the CIP-013 R 1.2.5 Requirement Part to provide additional clarity.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the conforming changes or scoping clarifications related to SCI made to the various CIP standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed conforming changes to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and thanks the SDT for their hard work in modifying the rest of the CIP Standards to allow for implementing future technologies while maintaining and even increasing security.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E supports the conforming changes to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
For the proposed CIP-008, the Applicability would include, "An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or Shared Cyber Infrastructure supporting a BES Cyber System." Note that by a literal reading of this, an SCI supporting EACMS would not be in scope for CIP-008 whereas a traditional EACMS would be.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. This appears to be a redlining issue. The working copy for Draft 5 showed the correct SCI applicability Statement.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
For the proposed CIP-008, the Applicability would include, "An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or Shared Cyber Infrastructure supporting a BES Cyber System." Note that by a literal reading of this, an SCI supporting EACMS would not be in scope for CIP-008 whereas a traditional EACMS would be.	

Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your comment. This appears to be a redlining issue. The working copy for Draft 5 showed the correct SCI applicability Statement.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
MPC supports comments that were submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
See response to MRO.	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	

Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the conforming changes and scoping clarifications made to CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	

Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
(1) The proposed language in in CIP-006-7, R1, Part 1.3, points to system capability, but there are concerns with situations where the PACS is capable, but there is a limitation with a particular physical access device. It seems as thought that may present a gap in the proposed language. As an example, an entity currently has a TFE for a limited physical access device where two factor cannot be applied, such as a roof hatch where it is not possible to install a locking mechanism controlled by the PACS system. Under the approved TFE, additional measures are taken to secure that physical access point. The concern with the proposed language is that the roof hatch may be seen as a physical access device rather than a system. In this instance, the PACS is capable of two-factor authentication, but two-factor authentication cannot be applied to that particular physical access device. Because of this potential and unintended gap, we recommend using the language “per system or device capability.” **(2) For CIP 009-7, Requirement R1, Part 1.1, please consider adding the language SCI supporting an Applicable System” in the Applicable Systems column**.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. CIP-006 R1.3 has been discussed extensively, and the SDT position is that the per system capability does apply at the system level, and the system is capable in the instance you present. However, there are components of the system that may not be, and the intent is to enforce the additional authentication method wherever components of the system support this capability.	

CIP-009's focus is to ensure that the BCS can be recovered. An Entity can choose to recover that functionality of the BCS in any manner that restores that functionality, potentially without the use of SCI, even if the original BCS included the use of SCI. Additionally, the majority of organizations making use of virtualization today will choose the All-In model where the underlay is classed as a part of the BCS itself. In this instance the underlay (not technically SCI) would be subject to the recovery requirements.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF	
Likes 0	
Dislikes 0	
Response	
See response to MRO NSRF.	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Israel Perez - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	

8. The SDT has revised the Implementation Plan to include 3 defined early adoption dates as options should Responsible Entities choose to do so. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
PNMR believes early adoption of the revised CIP standards and definitions is beneficial but proposes that Responsible Entities are not tied to only three early adoption choices (6, 12, or 18 months) after approval of the new standards. PNMR proposes that Responsible Entities still follow notifying their Regional Entities of their early adoption choice within fifteen calendar days of making that decision, but that Responsible Entities have the ability to early adopt at any time between 6 months and 24 months. If, for example, a Responsible Entity is not able to early adopt at the 6-month mark but would be able to 8 months after the approval of the new standards, the Responsible Entity should be able to early adopt and not have to wait an additional 4 months until the 12-month mark. An alternate proposal would be for the Responsible Entity to notify the Regional Entity of its 6, 12, or 18-month early adoption date but have the ability to change its early adoption date if it is realized before the agreed-upon early adoption date that the Responsible Entity would not be able to be compliant with the new standards by that date. In this case, the Responsible Entity could move its early adoption from 6 months to 12 months, for example.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The implementation plan allows for 3 specific early adoption dates that will be set to ensure that all entities are being held to the same date to reduce any confusion that may occur during any audits that may cross those periods. The SDT will add a clarifying note in the implementation plan.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment	
With the implementation of compliance oversight plans (COP)s, many entities, particularlylarger entities, are experiencing more frequent audits. 36 months may be more appropriate for an implmentation period based on the scope of the changes being proposed under this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT asserts that the existing 24 month time period is sufficient while considering the level of the backward compatible language that exists for most requirements. No changes were made to this longstanding portion of the language. It will carry forward from previously and currently approved versions of the implementation plan.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

EEI supports the revised Implementation Plan as proposed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Alison Mackellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
RF agrees with the inclusion of the 3 defined early adoption dates as options should Responsible Entities choose to do so with the understanding that all Standards and Requirements will be adopted at that same time.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the revised Implementation Plan and the three (3) defined early adoption dates.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Xcel Energy supports EEI comments and thanks the SDT for working on creating an implementation plan that will allow for enough time for a successful implementation while also allowing for early implementation for entities looking to employ virtualized technologies at a faster pace.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern understands and agrees with the revised implementation plan which includes 3 defined early adoption dates as an option. Southern also understands that if one of the options were chosen, we would have 15 calendar days to notify our Regional Entity of the selected option.	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
patricia ireland - DTE Energy - 4, Group Name DTE Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Wright - Sempra - San Diego Gas and Electric - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Diana Torres - Imperial Irrigation District - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC Regional Standards Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Wong - Seminole Electric Cooperative, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Ciufo - Mark Ciufo On Behalf of: Payam Farahbakhsh, Hydro One Networks, Inc., 3, 1; - Mark Ciufo	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cyntia Dore - Hydro-Qu?bec Production - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Steiner - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Benjamin Winslett - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
JT Kuehne - AEP - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Amazon Web Services - 7	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	

Answer	Yes
Document Name	
Comment	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
"See comments submitted by the Edison Electric Institute"	
Likes 0	

Dislikes 0	
Response	
See response to EEI.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE continues to be concerned there is conflicting language in the planned changes section of the implementation plan, as well as language in the unplanned changes section in the proposed implementation plan that could result in a reliability gap.

Regarding the conflicting language addressing planned changes, Texas RE notes that the second paragraph in the proposed implementation plan states: "For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation."

Texas RE understands this language to mean the BCS at the substation must be compliant upon the commissioning of the substation. Texas RE agrees with this position.

However, the first and third paragraphs in the proposed implementation plan appears to conflict with this reading. Specifically, the first paragraph states: "Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2." Furthermore, the proposed implementation plan's third paragraph states: "For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan."

Texas RE understands this language to mean the BCS at the substation is not required to be compliant until the Registered Entity has performed its annual assessment under CIP-002 R2. This introduces a reliability gap as assets that were commissioned shortly after the entity has completed a CIP-002 R2 evaluation will not be required to be evaluated for up to 15 calendar months, and therefore would not be required to be compliant with the applicable cyber security requirements. Texas RE does not agree with this position. Additionally, there are no requirements to identify PACS, EACMS, or PCAs.

Regarding the proposed implementation plan's concerning unplanned changes, Texas RE is concerned the language could be read to result in a reliability gap. Specifically, the first paragraph of the implementation plan states "Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2." Texas RE notes that while it is true that during a CIP-002 R2 review an entity may discover that a BCS now meets a higher BCS threshold than it previously held, this is not the only situation in which an entity may become aware of the need for a higher categorization. For example, if an entity is informed by their RC, PC, or TP that an asset is critical to the derivation of an IROL then the knowledge that the systems must meet the medium impact criteria is immediate and as such the 12-month timer to implement medium impact controls should begin immediately. As written, the language in the implementation plan could result in a situation where a Registered Entity could delay the implementation of medium impact controls at such a substation or power plant for up to 27 calendar months, if the IROL notification arrived immediately after a CIP-002 R2 evaluation. Texas RE recommends the SDT revise the proposed implementation plan language around "unplanned changes" to preclude this result.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. No changes have been made to this longstanding portion of the language. It will carry forward from previously and currently approved versions of the implementation plan. These changes are considered out of scope for the current 2016-02 project as it relates to Virtualization, IRA, or the remaining V5TAG items.	

9. Please provide any additional comments for the standard drafting team to consider, if desired.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
Southern suggests that the definition for "Cyber System" be modified to eliminate the "A group of" language and simply begin with "One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDTs modified the Cyber System definition.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nicholas Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	

Answer	
Document Name	

Comment

NST disagrees with the SDT decision to not compel Responsible Entities to identify and maintain a list of SCI that support BES Cyber Systems in CIP-002. In order to demonstrate compliance with various CIP-003 – CIP-013 requirements for SCI, a Responsible Entity would surely have to demonstrate that all its SCI were accounted for. NST is aware of the fact there is no existing CIP requirement to maintain an inventory of “associated” devices including PCAs, EACMS, and PACS, but doing so was some years ago memorably characterized by a well-known representative of a Regional Entity as an "implied requirement." NST believes an SDT goal should be to avoid adding to the list of "implied requirements."

NST believes the proposed “Exemption” statement in every CIP Standard, 4.2.3.3, “Cyber Systems, associated with communication links, between the Cyber Systems providing confidentiality and integrity of an Electronic Security Perimeter (ESP) that extends to one or more geographic locations” is both confusing and inaccurate. One provides for the confidentiality and integrity of data, not ESPs. N&ST suggests rewording that’s consistent with the language of proposed CIP-005 Requirement R1 Part 1.4, such as “Cyber Systems associated with communication links used to span a single ESP among two or more geographic locations.”

NST notes the second of two proposed "Measures" for CIP-007 R1 Part 1.3 suggests evidence of compliance with the "non-sharing" of SCI CPU and memory requirement could include "Hardware partitioning of physical Cyber Assets." If our understanding of "hardware partitioning" is correct (that it means, for example, all the Medium Impact BCS that co-reside with High Impact BCS on a single hardware platform are moved to different hardware), then according to the proposed definition of SCI, the end result of "hardware partitioning" would be one or more hardware platforms that are no longer SCI, which would render all proposed requirements for SCI, including CIP-007 R1 Part 1.3, inoperable.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Project 2021-03 Group B will look into the inclusion of the identification and maintenance of a list of SCI (and EACMS, PACS, and PCAs) that support BES Cyber Systems.

Exemption 4.2.3.3 intends to exclude the devices that may not be owned/operated by the Registered Entity, but carry the data between relevant locations which are all treated as a single ESP. This is necessary because the entity may have no ability to perform the required controls for these assets that would otherwise be considered in the same ESP as an applicable BCS. The control objective of the associated CIP-005 R1 Requirement is to ensure that this exclusion does not compromise the integrity or confidentiality of the data that traverses this link.

The Measures of CIP-007 R1 Part 1.3 second bullet inclusion of "Hardware Partitioning of physical Cyber Assets" may result in an entity creating an architecture that does not meet the new definition of SCI. It was included to cover the capabilities that systems like LPARs bring to the virtualization discussion, which offer advanced hardware partitioning capabilities initially implemented in the mainframe environment.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	
Document Name	
Comment	
AZPS has no additional comments for the standard drafting team to consider currently.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 6	
Answer	
Document Name	

Comment

We still have concerns on CIP-010-5 because the draft does not include the Guidelines and Technical Basis section where it defines what must be included in a vulnerability assessment. It is understood that the Standards Drafting team emphasizes backwards compatibility, but, the proposed changes to CIP-007 R1 and CIP-010 R1.1 could affect what is required in the vulnerability assessments. At the very least, we would like to know and comment on what additional items will be required for SCI in a vulnerability assessment as there is nothing found in the current proposed changes.

Lastly, under CIP-010 R3.3 BES Cyber System is shortened to BCS. However, this is different than the other parts of CIP-010 R3. We recommend consistency.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

The SDT investigated the option of re-introducing the guidance from the previous GTB section of CIP-010-3. This guidance section is in a CIP-010-4 Implementation Guidance document that was been submitted to the ERO for endorsement by the Project 2019-03 Drafting Team: https://www.nerc.com/pa/Stand/Project201903_Cyber%20Security%20Supply%20Chain%20Risks/2019-03_CIP-010-4_Implementation_Guidance_Redline_07282020.pdf

The SDT also addressed the inconsistency of acronym use within the Applicable Systems column within the Standard.

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	
Document Name	

Comment

Although not directly revised in this draft, two issues in CIP-007 deserve mention. Requirement 3.3 obstructs smooth updates of antimalware signatures with large administrative cost and compliance risk, for very little, if any, reliability benefit, and is actually impossible with many automated systems today. The requirement should be revised to remove the testing of signatures. Additionally, CIP-007 R5 language inherited from earlier versions requiring at least 8 character passwords is outdated. SIGE suggests requiring at least 15 character passwords, where capable.

Likes 0	

Dislikes 0	
Response	
Thank you for your comments. The issues raised are outside the scope of the Project 2016-02 SAR.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	
Document Name	
Comment	
None at this time.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	

Document Name	
Comment	
Although not directly revised in this draft, two issues in CIP-007 deserve mention. Requirement 3.3 obstructs smooth updates of antimalware signatures with large administrative cost and compliance risk, for very little, if any, reliability benefit, and is actually impossible with many automated systems today. The requirement should be revised to remove the testing of signatures. Additionally, CIP-007 R5 language inherited from earlier versions requiring at least 8 character passwords is outdated. CEHE suggests requiring at least 15 character passwords, where capable.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The issues raised are outside the scope of the Project 2016-02 SAR.	
Joe Gatten - Xcel Energy, Inc. - 1,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports EEI comments and would like to acknowledge the SDT for their hard work over the years in developing a very difficult and technological set of standards that allow for both backward compatibility and inclusion of future technologies.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. See response to EEI.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	

N/A	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Ed Hanson, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	
Document Name	
Comment	
PG&E wishes to thank the SDT for their several years of effort in getting these modifications close to completion.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Kendra Buesgens - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The proposed revised definition for EACMS would add the phrase, “Shared Cyber Infrastructure (SCI)” to the definition. The term “SCI” can refer to a system that is supporting PACS or EACMS. If the definition is read in terms of this type of SCI as it pertains to the EACMS definition, that opens the possibility that the scope of an EACMS could be read as applicable to Cyber Assets that perform electronic access control or monitoring of SCI “EACMS/PACS,” thus potentially creating a hall of mirrors effect. The MRO NSRF are not certain how probable or not such an interpretation may be,	

but prefer that this be addressed here rather than when it's too late to do so. The MRO NSRF ask that the SDT consider this issue and make any edits necessary to address.	
Likes 1	Lincoln Electric System, 1, Johnson Josh
Dislikes 0	
Response	
Thank you for your comment. The SDT appreciates the clarity you brought to the concern around the inclusion of SCI as a target of the controls found in the EACMS definition as it was in Draft 4 and modified the EACMS definition.	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	
Document Name	
Comment	
See comments provided by Mike Magruder and/or Glenn Farmer	
Likes 0	
Dislikes 0	
Response	
See response to Mike Magruder and/or Glenn Farmer.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Foung Mua, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; Wei Shao, Sacramento Municipal Utility District, 3, 5, 6, 4, 1; - Tim Kelley, Group Name SMUD / BANC	
Answer	
Document Name	
Comment	
The use of the terms routable protocol communications, bi-directional routable protocol connection and IP Protocol communications, throughout the standards and the definitions is inconsistent and should be evaluated to determine the necessity of using this different language. If providing the	

consistency through the standards is not an option, it would be better to put these into the definitions so that entities can differentiate one from the other.

The language in CIP-010 R1.1 appears to be getting further away from acceptable language with each iteration of the requirement. Moving requirements to the Measures column does not make the changes any more security objective focused.

Same comments for CIP-005 R1.2 in that the requirements to document a reason for routable protocol communications should be in the Requirements and not the Measures. Examples of the justification/reason are fine in the Measures, but the requirements should be in the Requirements column.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

The SDT was intentional in each use of the communications phrases, as each has a distinct implementation and impact based on the language used. There are some modifications to language in the applicable Requirements that may provide more clarity to the intended use. Additionally, the definition of IRA has been updated to include “bi-directional” in the latest draft as a result of this input. The SDT included this after determining that the concept was no longer included by way of the reliance on the External Routable Connectivity definition and is an integral part of Interactivity.

CIP-010 was the main focus of the Draft 5 changes, and working through the appropriate scoping of the change management processes was a key part of this. The SDT asserts that with the recent changes, the scoping is now at a valuable level to include those items that it should, and avoid those items appropriately. This language was drafted using input from many entities through outreach efforts and discussions with Trade Groups.

Thank you for your input on CIP-005 R1 Part 1.2. The SDT modified the Requirement language to clarify the need to include the reason for granting access.

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer	
Document Name	

Comment

WEC Energy Group is in agreement with the MRO NSRFs comment - "We also wish to raise attention to the proposed change of using the phrase “per system capability,” in place of the previous phrasing “where technically feasible.” While we do not wish for TFE to remain part of the compliance

paradigm any longer than necessary, we seek assurance that the phrase “per system capability” will indeed be used as an avenue for Registered Entities to demonstrate compliance instead of an opportunity for auditors to find fault with acceptable security and reliability practices."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. See response to MRO NSRF. The concept of "per system capability" is not new. See CIP-007-6 R4 Part 4.1 references to "per BES Cyber System" and "per Cyber Asset capability". The use remains the same, and the burden is on the Entity to document that the system is not capable of performing the required function, the same way the use is mentioned above from CIP-007-6 R4 Part 4.1.	
Meaghan Connell - Public Utility District No. 1 of Chelan County - 5, Group Name PUD No. 1 of Chelan County	
Answer	
Document Name	
Comment	
Chelan asks the SDT to consider the real risks and the goals of the CIP standards. CIP has always been about the protection of BES Cyber Assets/Systems and reducing the risk of a compromise or failure of a BES Cyber System which would adversely impact the BES. By definition, BES Cyber Systems are systems that will have direct impact on the BES, so it makes sense to protect those devices most stringently. Protected Cyber Assets also represent a significant risk since there is no network separation between PCAs and their associated BES Cyber System. A VM escape attack executed against a BES Cyber System would be a single exploit to potentially adversely impact the BES. However, EACMS and PACS devices do not have a direct impact on the reliability of the BES, and are segregated from BES Cyber Systems and Protected Cyber Assets by protections required by CIP-005. A successful VM escape against a EACMS or PACS device would require a second attack for there to be an adverse impact to the BES. The new affinity requirements increase both the risk of an adverse impact, by reducing the availability of the in-scope VMs and increase the risk of non-compliance, by forcing the use of a control not meant for this purpose. The requirements proposed essentially create six groups of devices that potentially may not share CPU or memory: 1) High Impact BCS/PCA (including EACMS and PACS classified as PCAs, excluding Intermediate Systems)	

2) High Impact EACMS/PACS (outside the ESP)

3) Medium Impact BCS/PCA (including EACMS and PACS classified as PCAs, excluding Intermediate Systems)

4) Medium Impact EACMS/PACS (outside the ESP)

5) Potentially Low Impact BCS

6) Out-of-Scope Devices

This means that a RE would have to establish up to 6 separate resource pools to comply with the definition of PCA and the text of CIP-007 R1.3. Assuming you can group devices in the affinity rule sets you create (this may not be possible on all platforms), this would require 15 separate anti-affinity rules, in addition any existing rules required for resource management purposes.

With the updated language suggested in Question 4, there would only be 3 resource pools needed:

1) High Impact BCS/PCAs (including EACMS and PACS classified as PCAs, excluding Intermediate Systems

2) Medium Impact BCS/PCA (including EACMS and PACS classified as PCAs, excluding Intermediate Systems)

3) All other devices.

Only 3 anti-affinity rules are needed here to satisfy the suggested requirements. This greatly reduces the complexity of the DRS rules needed to satisfy the security objective to protect the BES from the threat of VM escape attacks and decreases the risk of that a BES Cyber System is unable to find a host to run in the event of a failure of one or more SCI hosts.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

The SDT made changes to the affinity requirements with the intent to create two pools of resources that should not cross where mixed trust exists without high watermarking. Specifically, resources associated with High or Medium Impact BCS or their associated EACMS, PACS or PCA, would be in one pool and Low Impact BCS and non-CIP systems would be in another resource pool. This should simplify the implementation, while maintaining the security benefit that isolating our most critical systems from those less trusted.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	
Document Name	
Comment	
MPC supports comments that were submitted by the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
See response to MRO NSRF.	
Kristine Martz - Amazon Web Services - 7	
Answer	
Document Name	
Comment	
The SDT is clear that this project SAR focuses on on-premise virtualization, however, many virtualization concepts convey use of cloud. AWS suggests explicitly stating whether these new terms/requirements, specifically SCI, will apply to cloud or not. If these terms/requirements do not apply to cloud, it should be obvious to the reader.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SAR does not include an overall look at CIP standards for situations where Cyber Systems are owned/operated by non-registered entities. The SDT is simply defining what SCI is. There is a possibility the definition will apply to infrastructure not owned/operated by the registered entity, when the Standards are modified to provide for this capability in the future.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	

Document Name	
Comment	

Conflating support for both High-, Medium-, and Low-Impact Cyber Assets within a single Virtualization Cluster will create additional questions and interpretations between Responsible Entities and ERO Enterprise staff. Clusters by their very nature include pools of shared SCI to include CPU, Memory, Disk, and network resources that are shared between all Cluster members to allow for balancing resources, recovery from failed hardware, and maintaining high availability. The complexity required to balance these pooled resources using affinity rules or logical boundaries to disallow different impact levels of VM guests from running on the same physical resources could be high. Moving VM guests can take place without the need for clustering and would allow for segregated siloing of different impact Cyber Assets without the requirement of determining high-water marking every time a VM guest is moved. Communications play a key role in determining the current health and configuration of clusters – especially with heartbeats and SCSI data requests. Responsible Entities have a high bar to assure that these communications are not to the point that they create common networking connections that would start to include additional VM Guests as PCA.

Marrying both ESP and zero-trust within an overall ESP would better serve our Responsible Entities and create a more secure environment as zero-trust Cyber Assets would not be internet-facing while simplifying the management of the environment. Maintaining the ESP, and fully incorporating virtualization and zero trust paradigms within an identified ESP allows Responsible Entities to leverage another layer of defense (defense-in-depth) for BCS by limiting ingress/egress points and access to these Cyber Assets.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

The SDT made changes to the affinity requirements with the intent to create two pools of resources that should not cross where mixed trust exists without high watermarking. Specifically, resources associated with High or Medium Impact BCS or their associated EACMS, PACS or PCA, would be in one pool and Low Impact BCS and non-CIP systems would be in another resource pool. This should simplify the implementation, while maintaining the security benefit that isolating our most critical systems from those less trusted.

The current definition and requirement language in Draft 5 is meant to allow both the old boundary based ESP and modern zero-trust architectures, without precluding one or the other. Requiring a boundary based ESP is counter to zero-trust, since it is applied as close to the affected processes as possible, and everywhere there is an enforcement point in between.

Todd Bennett – Associated Electric Cooperative, Inc. – 3, Group Name AECI

Answer	

Document Name	
Comment	
"Responsible Entity" is used multiple times in the CIP standards and is not a defined term or a proposed defined term. The standard drafting team may consider defining this term in the NERC Glossary of Defined Terms. AECI supports the efforts and commitment of the standards drafting team to 296industry when soliciting feedback and proposing solutions to identified gaps in the draft standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Responsible Entity is defined in Section 4.1 at the top of the Standards.	
Alison Mackellar - Constellation - 5	
Answer	
Document Name	
Comment	
Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	

Kimberly Turco, on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends clear and concise language on the categorization and impact rating the hosting virtualization infrastructure should have. Specifically, Texas RE recommends eliminating the Shared Cyber Infrastructure definition. Virtualization infrastructure should inherit the highest impact rating and categorizations of the VCAs that the virtualization infrastructure is hosting. For example, if virtualization infrastructure is hosting two high impact BCS, three PCAs associated with high impact BCS, and an EACMS associated with high impact BCS, then the virtualization	

infrastructure should be categorized as a high impact BCS. Implementing high watermarking practices would ensure that the virtualization infrastructure is more reliable and secure. Texas RE continues to note that no matter how many controls are applied there will always be a parent and child relationship between host and VM's. If the hypervisor is compromised, then all VM's can be. Additionally, if a VM is compromised the same can be true, other VM's and the Hypervisor can be impacted. The Hypervisor should be high watermarked to whatever VMs are on it. Any VMs on the hypervisor should also be marked at the highest impact rating. Different applicable systems with varying impact level lends itself to mixed-trust concepts. This change potential opens the door to allow more corporate based systems (payroll, custom software, etc.) to be on the same hypervisor as CIP applicable systems. CPU and memory segregation only may not protect from vulnerabilities such as hyperjacking, VM escape, Denial of Service, etc.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Applicable Systems insertion of "SCI supporting an Applicable System in this Part" enforces a High Watermark for the SCI itself. This SCI statement is cascaded throughout the CIP Standards with only a few exceptions, where the requirement language does not support the inclusion. If there are significant deviations in treatment which do not support this, the SDT would like to be made aware of them.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	

Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
See response to EEI.	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
See Response to EEI.	
Jodirah Green - ACES Power Marketing - 6	
Answer	
Document Name	
Comment	
We would like to thank the Project 2016-02 SDT on their hard work, dedication, and continuing to listen to industry feedback to meet the FERC order and not create significantly more compliance burden.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Diana Torres - Imperial Irrigation District - 6	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	
Document Name	
Comment	
It is unclear in the draft CIP-002-7 how the classification hierarchy is impacted. What is the hierarchy of the SCI classification? Is dual classification with SCI expected??	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. See the CIP-002 TR and Definitions Rationale for how the hierarchy is applied to SCI. In essence this is applied through the inclusion of "SCI supporting an Applicable System in this Part".	

Wesley Maurer - Wesley Maurer On Behalf of: Teresa Krabe, Lower Colorado River Authority, 5, 1; - Wesley Maurer	
Answer	
Document Name	
Comment	
LCRA would like to seek clarification regarding virtualization of EACMS outside of an ESP. If the host has in-scope EACMS as well as out of scope virtualized machines, would the same rules apply as SCI within a the ESP? There would be SCI associated with an EACMS. There would be an EACMS that is a virtual machine. Are affinity rules the only compliance obligation associated with the out of scope VM?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Referring to the Applicable System column within the CIP Standards where the phrase "SCI supporting an Applicable System in this Part" exists and an SCI supports an EACMS associated with either the HIBCS, or some form of MIBCS, the requirements apply to both the EACMS and SCI that support it. This applies to the Affinity requirement as well as Applicable Systems, not the out of scope VM. However, applying an affinity rule to Applicable VMs would enforce an anti-affinity rule for out of scope VMs by practice.	
James Baldwin - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	
LCRA would like to seek clarification regarding virtualization of EACMS outside of an ESP. If the host has in-scope EACMS as well as out of scope virtualized machines, would the same rules apply as SCI within a the ESP? There would be SCI associated with an EACMS. There would be an EACMS that is a virtual machine. Are affinity rules the only compliance obligation associated with the out of scope VM?	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment. Referring to the Applicable System column within the CIP Standards where the phrase "SCI supporting an Applicable System in this Part" exists and an SCI supports an EACMS associated with either the HIBCS, or some form of MIBCS, the requirements apply to both the EACMS and SCI that support it. This applies to the Affinity requirement as well as Applicable Systems, not the out of scope VM. However, applying an affinity rule to Applicable VMs would enforce an anti-affinity rule for out of scope VMs by practice.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) 2016-02 Virtualization (Draft 4)	
Answer	
Document Name	
Comment	
In future postings, for definitions, it would be helpful if the table for the definitions could include each standard where the definition appears. *In closing, SRC reiterates that our gravest concern is with proposed changes to CIP-010, Part 1.1 and Part 2.1 which do away with the concept of "baseline changes." The proposed language of "settings changes" goes beyond what was previously in the CIP standards such that we believe they are no longer backwards compatible. SRC proposes "settings changes" be modified to "configuration changes" or eliminated altogether.* *Additionally, the SRC would like for the SDT to consider that the standards process has taken very long and there are newer technologies that are not being addressed with these changes.*	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Definitions Table has been modified to include references to where the definition is used. The language of CIP-010 R1 was the main focus of the Draft 5 changes. See the revised language which makes use of the "configuration changes" concept.	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	

Alliant Energy supports the comments submitted by the MRO NSRF	
Likes 0	
Dislikes 0	
Response	
See response to MRO NSRF.	

End of Report

Agenda Item 6
Standards Committee
October 19, 2022

Project 2016-02 Modifications to CIP Standards

Action

Approve the following waiver of provisions of the Standard Processes Manual (SPM) for Project 2016-02 Modifications to CIP Standards:

- Additional formal comment and ballot period(s) reduced from 45 days to as few as 20 calendar days with ballot(s) conducted during the last 5 days of the comment period. (Sections 4.9 and 4.12)
- Final ballot period reduced from 10 days to as few as 5 calendar days. (Section 4.9)

Background

Section 16.0 of the SPM allows the Standards Committee to waive any provision in the SPM for good cause, including for the following reason:

> *Where the Standards Committee determines that a modification to a proposed Reliability Standard or its Requirement(s), a modification to a defined term, a modification to an Interpretation, or a modification to a Variance has already been vetted by the industry through the standards development process or is so insubstantial that developing the modification through the processes contained in this manual will add significant time delay.*

NERC Project 2016-02 Modifications to CIP Standards has completed four ballots to date. Each ballot consisted of CIP-002 through CIP-011 and CIP-013 Reliability Standards, the associated definitions for inclusion in the *NERC Glossary of Terms used in Reliability Standards*, and the associated Implementation Plan. Prior to these formal comment periods, the Standard Drafting Team (SDT) conducted significant informal outreach since the inception of the project to gather industry feedback.

Given the stage of development and the content of the comments, the SDT anticipates only making targeted revisions based on comments received over the course of these comment periods. As such, the future proposed changes will have received significant vetting through the comment periods and informal outreach by the team and the waivers will permit the SDT and industry to complete this project without further delay.

As background, the initial comment period and ballot was conducted January 22 – March 22, 2021, which failed to achieve the necessary consensus for approval. The second comment period and ballot was conducted from June 30 – September 1, 2021, which similarly failed to achieve the necessary consensus for approval. The third comment period and ballot was conducted from February 18 – April 12, 2022, in which CIP-002, CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013 passed ballot and CIP-005, CIP-007, and CIP-010 failed ballot. The fourth comment period and ballot was conducted from August 17 – October 7, 2022, in which CIP-002, CIP-003, CIP-004, CIP-006, CIP-007, CIP-008, CIP-009, CIP-011, and CIP-013 passed ballot and CIP-005 and CIP-010 failed ballot.

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Minutes
Standards Committee Meeting

October 19, 2022 | 1:00—3:00 p.m. Eastern

Amy Casuscelli, chair, called to order the meeting of the Standards Committee (SC or the Committee) on October 19 at 1:00 p.m. Eastern. A. Oswald, secretary, called roll and determined the meeting had quorum. The SC member attendance and proxy sheets are attached as Attachment 1.

NERC Antitrust Compliance Guidelines and Public Announcement
The Committee secretary called attention to the NERC Antitrust Compliance Guidelines and the public meeting notice and directed questions to NERC's General Counsel, Sonia C. Mendonça.

Introduction and Chair's Remarks
Amy Casuscelli welcomed the committee, guests, and proxies to the meeting. S. Kelly remarked that the NERC Board of Trustees has an open meeting on October 26, 2022 to consider the draft cold weather standards from Project 2021-07. In addition, the Board of Trustees is seeking policy input on the standards process improvements to help streamline the pace of development without sacrificing ANSI standards for open development.

Review October 19, 2022 Agenda (agenda item 1)
The committee approved the October 19 meeting agenda.

Consent Agenda (agenda item 2)
The committee approved the September 21, 2022 SC Meeting Minutes.

Projects Under Development (agenda item 3)
C. Yeung reviewed the Project Tracking Spreadsheet. L. Harkness reviewed the Projected Posting Schedule.

Project 2021-06 Modifications to IRO-010 and TOP-003 (agenda item 4)
J. Mallory provided an overview. S. Rueckert made a motion to authorize initial posting of proposed Reliability Standards IRO-010-5 and TOP-003-6 and the associated Implementation Plan for a 45-day formal comment period, with ballot pool formed in the first 30 days, and parallel initial ballots and non-binding polls on the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), conducted during the last 10 days of the comment period.

The committee approved the motion with no objections or abstentions.

Project 2021-02 Modifications to VAR-002-4.1 (agenda item 5)
L. Harkness provided an overview. P. Winston made a motion to authorize initial posting of proposed Reliability Standard VAR-002-5 and the associated Implementation Plan for a 45-day formal comment

period, with ballot pool formed in the first 30 days, and parallel initial ballot and non-binding polls for the Violation Risk Factors and Violation Severity Levels, conducted during the last 10 days of the comment period.

The committee approved the motion with no objections or abstentions.

Project 2016-02 Modifications to CIP Standards (agenda item 6)
L. Harkness provided an overview. S. Rueckert stated that the reduced final ballot could end on a weekend. L. Harkness stated that NERC staff does not allow ballots to end on a weekend and if the schedule fell like that it would be extended to end the following week. L. Oelker asked what the need was for the reduced comment periods. L. Harkness stated that this project has had four ballots with an improved approval rate on each ballot with much industry vetting. The team is making targeted changes based on industry feedback and therefore NERC believes that industry could review those changes in a shorter time period allowing the project to complete and allocate NERC and industry resources to other projects. C. Yeung and P. Winston state that they do not see this explanation as a reason to shorten the comment and ballot periods as stated in the waiver. J. Johnson stated a concern that a shortened comment period could actually result in more negative votes. M. Jones stated he shared these concerns, but thinks the SC should trust the team and NERC developers as this is the course of action that is being recommended. He also states he does not believe that the team would go as low as a 20-day comment period but advocates for approving the waiver and letting the team make that decision. P. Winston stated he could support a reduced additional comment and ballot period, but does not support the reduced final ballot period. P Winston made a motion to approve the following waiver of provisions of the Standard Processes Manual (SPM) for Project 2016-02 Modifications to CIP Standards: additional formal comment and ballot period(s) reduced from 45 days to no less than 20 calendar days with ballot(s) conducted during the last 10 days of the comment period. M. Hostler stated his primary concern is with CIP-010 and asked what changes are going to be made to that standard. In addition, he asked if final ballots for the standards would occur together or separate. L. Harkness stated that each standard has been balloted individually thus far and they will continue to be balloted individually for final ballot. In addition she stated that the changes being made to CIP-010 by the drafting team are a technical issue and not a subject the SC should be discussing. M. Hostler asks if this waiver will shorten the time the drafting team has to do revisions to prepare for the next comment and ballot. L. Harkness stated it will not.

The committee approved the motion. J. Johnson objected and C. Yeung abstained.

2023-2024 Term Elections (agenda item 7)
A. Oswald notified the committee that the nomination period for the 2023-2024 SC term elections are currently open. Anyone interested in submitting a nomination should do so before the end of the of the nomination period.

Registered Ballot Body Update (agenda item 8)
M. Hecht provided an overview on the changes to the Registered Ballot Body.

Legal Update and Upcoming Standards Filings (agenda item 9)
M. Hecht provided the legal update regarding recent and upcoming filings.

Adjournment

A. Casuscelli adjourned the meeting at 1:55 p.m. Eastern.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Committee
2022 Segment Representatives

Segment and Terms	Representative	Organization	Proxy	Present (Member or Proxy)
Chair 2022-23	Amy Casuscelli Manager, Reliability Assurance & Risk Management	Xcel Energy		x
Vice Chair 2022-23	Todd Bennett Managing Director, Reliability Compliance & Audit Services	Associated Electric Cooperative, Inc.		x
Segment 1-2022-23	Michael Jones Manager, Reliability Standards & Policy	National Grid		x
Segment 1-2021-22	Troy Brumfield Regulatory Compliance Manager	American Transmission Company		x
Segment 2-2022-23	Jamie Johnson Compliance Analyst Lead – RC Operations	California ISO		x
Segment 2-2021-22	Charles Yeung Executive Director Interregional Affairs	Southwest Power Pool		x
Segment 3-2022-23	Kent Feliks Manager NERC Reliability Assurance – Strategic Initiatives	American Electric Power Company, Inc.		x
Segment 3-2021-22	Linn Oelker Manager – Market Compliance	LG&E and KU Services Company		x
Segment 4-2022-23	Marty Hostler Reliability Compliance Manager	Northern California Power Agency		x
Segment 4-2021-22	Alice Wright Senior Director, Compliance Services	Arkansas Electric Cooperative Corporation		x
Segment 5-2022-23	Terri Pyle Utility Operational Compliance and NERC Compliance Office	Oklahoma Gas and Electric		x
Segment 5-2021-22	Jim Howell Markets Compliance Manager	Southern Company Generation		x

Segment and Terms	Representative	Organization	Proxy	Present (Member or Proxy)
Segment 6-2022-23	Sarah Snow* Manager of Reliability Compliance	Cooperative Energy		x
Segment 6-2021-22	Justin Welty Senior Manager, NERC Reliability Standards	NextEra Energy	Silvia Parada-Mitchell	x
Segment 7-2022-23	Kristine Martz Industry Specialist, Power & Utilities	Amazon Web Services		x
Segment 7-2021-22	Venona Greaff* Senior Energy Analyst	Occidental Chemical Corporation		x
Segment 8-2022-23	Robert Blohm[1] Managing Director	Keen Resources Ltd.		n
Segment 8-2021-22	Philip Winston* Retired (Southern Company)	Independent		x
Segment 9-2022-23	Sarosh Muncherji Cyber Security Specialist	British Columbia Utilities Commission		x
Segment 9-2021-22	William Chambliss General Counsel	Virginal State Corporation Commission		n
Segment 10-2022-23	Tony Purgar Manager, Operational Analysis & Awareness	ReliabilityFirst		x
Segment 10-2021-22	Steven Rueckert Director of Standards	WECC		x

---

[1] Serving as Canadian Representative
*Denotes SC Executive Committee Member

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 5 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-10

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-10:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that

include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with mandatory and enforceable Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	within 18 calendar months of the previous approval. (R1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-003-10)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2)
OR
The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2)
OR
The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2)
OR
The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)</td><td>controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2)
OR
The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2)
OR
The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (R2)
OR
The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2)
OR
The Responsible Entity failed to document the determination of whether an</td><td>according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2)
OR
The Responsible Entity documented failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2)
OR
The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)
OR
The Responsible Entity failed to implement mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)</td><td></td></tr>
</table>

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber process for vendor electronic remote access security controls according to	

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (R2)	Requirement R2, Attachment 1, Section 6. (R2)	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	TBD	Modified by Project 2016-02	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process

documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. <u>TCA and Removable Media Malicious Code Risk Mitigation</u>:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
   - steps to preauthorize access;
   - alerts generated by vendor log on;
   - session monitoring;
   - security information management logging alerts;
   - time-of-need session initiation;
   - session recording;
   - system logs; or
   - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
   - disabling vendor electronic remote access user or system accounts;
   - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
   - disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;

    - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
    - administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
    - other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - alerting; or
    - other operational, procedural, or technical controls.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 5 Definitions".

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-10

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-10:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates: See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that

include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with mandatory and enforceable Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	within 18 calendar months of the previous approval. (R1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the determination of whether an	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber process for vendor electronic remote access security controls according to	

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (R2)	Requirement R2, Attachment 1, Section 6. (R2)	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	TBD	Modified by Project 2016-02	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact BCS within the asset; and
  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process

documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - security information management logging alerts;
    - time-of-need session initiation;
    - session recording;
    - system logs; or
    - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
    - disabling vendor electronic remote access user or system accounts;
    - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
    - disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;

  - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
  - administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
  - other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - alerting; or
    - other operational, procedural, or technical controls.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~fourth~~fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – ~~September 30~~October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	~~October 2022~~November 2023
Board adoption	~~November 2022~~December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft ~~4~~5 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-~~Y~~10

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.
~~All BES Facilities.~~

4.2.3. Exemptions: The following are exempt from Standard CIP-003-~~Y~~10:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links~~,~~ between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation;~~ and~~

1.2.6. Vendor electronic remote access security controls; and

~~**1.2.6.**~~**1.2.7.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that

include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity~~, or any entity as otherwise designated by an Applicable Governmental Authority,~~ in their respective roles of monitoring and~~/or~~ enforcing compliance with mandatory and enforceable Reliability Standards~~ in their respective jurisdictions~~.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-~~Y~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-~~Y~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the ~~six~~seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the ~~six~~seven topics required by R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the ~~six~~seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the ~~six~~seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager

R #	**Violation Severity Levels (CIP-003-~~Y~~10)**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	within 18 calendar months of the previous approval. (R1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-~~Y~~10)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the determination of whether an	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	

R #	Violation Severity Levels (CIP-003-~~Y~~10)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment	OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber process for vendor electronic remote access security controls according to	

R #	Violation Severity Levels (CIP-003-~~Y~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (R2)	Requirement R2, Attachment 1, Section 6. (R2)	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-~~Y~~10)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	TBD	Modified by Project 2016-02	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For ~~TTCA~~TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- ~~Controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;~~
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;

- ~~Review of controls that maintain the state of the operating system and software such that they are in a known state prior to execution that mitigates the risk of introduction of malicious code;~~
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
    a. The asset, if any, or the locations of the low impact BCS within the asset; and
    b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process

documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, ~~controls to maintain the known good state of the OS and software,~~ application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of ~~controls to maintain the known good state of the OS and software, or~~ system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the

party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
   - steps to preauthorize access;
   - alerts generated by vendor log on;
   - session monitoring;
   - security information management logging alerts;
   - time-of-need session initiation;
   - session recording;
   - system logs; or
   - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
   - disabling vendor electronic remote access user or system accounts;
   - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
   - disabling communications protocols (such as IP) used for

systems which establish and/or maintain vendor electronic remote access;

- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:

   - Anti-malware technologies;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Automated or manual log reviews;
   - alerting; or
   - other operational, procedural, or technical controls.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 5 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls
2. **Number:** CIP-003~~-9~~-10
3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

~~**1.1.**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003~~-9~~-10:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (~~ESPs~~ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~5.~~ **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan ~~for CIP-003-9~~

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact ~~BES Cyber Systems~~BCS, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of ~~BES Cyber Systems~~BCS (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for ~~BES Cyber Systems~~BCS (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP~~-~~-002 containing low impact ~~BES Cyber Systems~~BCS shall implement one or more documented cyber security plan(s) for its low impact ~~BES Cyber Systems~~ BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact ~~BES Cyber Systems~~BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with ~~the NERC~~mandatory and enforceable Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non~~-~~-compliant, it shall keep information related to the non~~-~~-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records~~,~~ and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 15 calendar months but did	did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one	required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 within	Systems as required by ~~R1.~~ ~~(R1~~Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by R1. (R1.2) OR The Responsible Entity did not complete its ~~review~~approval of the one or more documented ~~cyber security policies~~ cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BES Cyber Systems as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	months of the previous approval. (R1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2)	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2)	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2)	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	OR The Responsible Entity failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to manage its	OR The Responsible Entity failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2)	OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (R2)	

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	OR The Responsible Entity failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according	OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for TCA managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior	

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (R2)	to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (R2)	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from ~~–~~-2 to ~~–~~-3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP~~–~~-003~~–~~-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

~~Version~~	~~Date~~	~~Action~~	~~Change Tracking~~
			~~Order No. 791 related to identify, assess, and correct language and communication networks.~~
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP~~-~~-003~~-~~-6. Docket No. RM15~~-~~-14~~-~~-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP~~-~~-003~~-~~-7. Docket No. RM17~~-~~-11~~-~~-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP~~-~~-003~~-~~-8. Docket No. RD19~~-~~-5~~-~~-000.	

~~Version~~	~~Date~~	~~Action~~	~~Change Tracking~~
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP~~-~~-003~~-~~-9. Docket No. RD23-3~~-~~-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	TBD	Modified by Project 2016-02	

~~Attachment~~

Attachment 1

Required Sections for Cyber Security Plan(s) ~~for Assets Containing Low Impact BES Cyber Systems~~

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple~~-~~-impact ~~BES Cyber Systems~~BCS ratings can utilize policies, procedures, and processes for their high or medium impact ~~BES Cyber Systems~~BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. ~~Section 1.~~ Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. ~~Section 2.~~ Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset, and (2) the Cyber Asset(s~~),~~) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. ~~Section 3.~~ Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP~~-~~-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. ~~between~~Between:

- a low impact ~~BES Cyber System(s)~~ BCS; or
- An SCI that supports a low impact BCS

and a Cyber ~~Asset~~System(s) outside the asset containing ~~low impact BES Cyber System(s);~~:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

~~i.~~ii. using a routable protocol when entering or leaving the asset containing the low impact ~~BES Cyber System(s);~~BCS or SCI that supports a low impact BCS; and

~~ii.~~iii. not used for time~~-~~-sensitive ~~protection or control functions between intelligent electronic devices (e.g.,~~ communications ~~using protocol IEC TR-61850-90-5 R-GOOSE).~~of Protection Systems.

3.2 Authenticate all Dial~~-~~-up Connectivity, if any, that provides access to low impact ~~BES Cyber System(s),~~BCS or SCI that supports a low impact BCS, per ~~Cyber Asset~~system capability.

Section 4. ~~Section 4.~~ Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E~~-~~-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. ~~Transient Cyber Asset~~ TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact ~~BES Cyber Systems~~BCS, through the use of ~~Transient Cyber Assets~~TCA or Removable Media. The plan(s) shall include:

5.1 For ~~Transient Cyber Asset(s)~~TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on~~-~~-demand manner (per ~~Transient Cyber Asset~~TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting ~~the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset~~(per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;

Commented [A1]: Rejected deletion.

- Review of system hardening used by the party; or
- ~~Other~~Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset.~~TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a ~~BES Cyber System~~BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~BCS or SCI that supports a low impact BCS.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

~~6.1~~ **6.3** One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) ~~for Assets Containing Low Impact BES Cyber Systems~~

Section 1. ~~Section 1.~~ Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e~~-~~-mails, memos, or computer~~-~~-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. ~~Section 2.~~ Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset; and
  b. The Cyber ~~Asset~~System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. ~~Section 3.~~ Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets ~~containing low impact BES Cyber Systems,~~ , the routable protocol communication ~~between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset~~as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that ~~communication is~~communications are used for time~~-~~-sensitive ~~protection or control functions between intelligent electronic devices~~communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) ~~between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s)~~ or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial~~-~~-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial~~-~~-back modems, modems that must be remotely controlled by the control center or control room, or access control on the ~~BES Cyber System~~BCS).

Section 4. ~~Section 4.~~ Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E~~-~~-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. ~~Section 5.~~ ~~Transient Cyber Asset~~TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

   Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of ~~live operating systems or~~ system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

2. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on~~-~~-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code~~.~~

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - security information management logging alerts;
    - time-of-need session initiation;
    - session recording;
    - system logs; or
    - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
    - disabling vendor electronic remote access user or system accounts;

  - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
  - disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
  - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
  - administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
  - other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - alerting; or
    - other operational, procedural, or technical controls.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 5 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-8

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.

4. **Applicability:**

    4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

        4.1.1. **Balancing Authority**

        4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

            4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

                4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

                4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

            4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

            4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

            4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

        4.1.3. **Generator Operator**

        4.1.4. **Generator Owner**

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-004-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part.	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS with IRA SCI supporting an Applicable System in this Part	months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS with IRA SCI supporting an Applicable System in this Part		
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP) (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual’s ability for unescorted physical access (except for Medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual’s authorized electronic access to individual accounts; and authorized unescorted physical access (except for Medium impact BCS without ERC) that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Examples of evidence may include, but are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	Examples of evidence may include, but are not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: - List of authorized individuals; - List of individuals who have been provisioned access; - Verification that provisioned access is appropriate based on need; and - Documented reconciliation actions, if any.
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a Medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	authorized unescorted physical access. (Part 2.2) OR The Responsible Entity did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for two individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1)	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)
R5	The Responsible Entity did not revoke individual's user accounts upon termination action within 30 calendar days of the date of	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	termination action for one or more individuals. (Part 5.3) OR The Responsible Entity did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	within 24 hours of the termination action for one individual. (Part 5.1) OR The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	complete the removal within 24 hours of the termination action for two individuals. (Part 5.1) OR The Responsible Entity for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action for three or more individuals. (Part 5.1) OR The Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (Requirement R6) OR The Responsible Entity, for four or more individuals, did not authorize provisioned electronic access to

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not perform the verification required by Part 6.2 within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for one individual, did not remove the individual’s ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for two individuals, did remove each individual’s ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for three individuals, did not remove each individual’s ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for four or more individuals, did not remove each individual’s ability to use provisioned access to BCSI by the timeframe required in Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
8	TBD	Modified by Project 2016-02.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~fourth~~fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – ~~September 30~~October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	~~October 2022~~November 2023
Board adoption	~~November 2022~~December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft ~~4~~5 Definitions".

A.- Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-8

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.

4. **Applicability:**

    4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” -For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. **Balancing Authority**

    4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. **Generator Operator**

    4.1.4. **Generator Owner**

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-004-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B.- Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R1 – Security Awareness Program

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part.	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. -Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-8 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months~~.~~ (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS with IRA SCI supporting an Applicable System in this Part	months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s criteria or process to evaluate criminal history records checks.
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity’s criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-8 Table R3 – ~~-~~Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
	Medium impact BCS with IRA SCI supporting an Applicable System in this Part		
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP~~).~~) (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the

CIP-004-8 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
			verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access (except for Medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts; and authorized unescorted physical access (except for Medium impact BCS without ERC) that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Examples of evidence may include, but are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-8 Table R5 – ~~-~~Access Revocation

Part	Applicable Systems	Requirements	Measures
5.3	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	Examples of evidence may include, but are not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI~~.~~ (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: - List of authorized individuals; - List of individuals who have been provisioned access; - Verification that provisioned access is appropriate based on need; and - Documented reconciliation actions, if any.
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a Medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C.- Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance.- For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	authorized unescorted physical access. (Part 2.2) OR The Responsible Entity did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for two individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1)	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)
R5	The Responsible Entity did not revoke individual’s user accounts upon termination action within 30 calendar days of the date of	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	termination action for one or more individuals. (Part 5.3) OR The Responsible Entity did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	within 24 hours of the termination action for one individual. (Part 5.1) OR The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	complete the removal within 24 hours of the termination action for two individuals. (Part 5.1) OR The Responsible Entity for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action for three or more individuals. (Part 5.1) OR The Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. -(Part 6.1) OR	The Responsible Entity, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. -(Part 6.1) OR	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. -(Requirement R6) OR The Responsible Entity, for four or more individuals, did not authorize provisioned electronic access to

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	The Responsible Entity did not perform the verification required by Part 6.2 within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for one individual, did not remove the individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for two individuals, did remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for three individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for four or more individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
8	TBD	Modified by Project 2016-02.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 5 Definitions".

A. Introduction

1. **Title:** Cyber Security — Personnel & Training
2. **Number:** CIP-004-~~7~~8
3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting ~~BES Cyber Systems~~BCS.
4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. **Balancing Authority**

4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. **Generator Operator**

4.1.4. **Generator Owner**

4.1.5. **Reliability Coordinator**

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~7~~8:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002~~-5.1a~~ identification and categorization processes.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan" ~~for CIP-004-7~~.

~~6. **Background:** Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could~~

~~meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~**” Columns in Tables:**~~

~~6.1.~~5.1. **”:** Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies. ~~The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~7~~8 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES~~impact BCS Medium impact BCS Shared Cyber ~~Systems~~Infrastructure (SCI) supporting an Applicable System in this Part. ~~Medium Impact BES Cyber Systems~~	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to ~~BES Cyber~~Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. ~~-~~Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~7~~8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~7~~8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~7~~8 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
2.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS~~;~~); and 2. Physical Access Control Systems (PACS)~~PACS~~ Medium ~~Impact BES Cyber Systems~~ impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for ~~BES Cyber Systems~~BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a ~~BES Cyber System's~~BCS electronic interconnectivity and interoperability with other Cyber ~~Assets~~Systems, including Transient Cyber Assets~~,~~ (TCA), and	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~7~~8 Table R2 – ~~-~~Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
		with Removable Media.	
2.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to ~~applicable Cyber Assets~~Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months~~.~~ (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated individual training records.

CIP-004-~~7~~8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS with IRA SCI supporting an Applicable System in this Part		

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to ~~BES Cyber~~Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber~~	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High ~~Impact BES Cyber Systems~~impact	Criteria or process for verifying that	~~An e~~Example of evidence may include, but

CIP-004-~~7~~8 Table R3 – ~~-~~Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
	BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	~~is~~are not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.
3.5	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 ~~to~~through 3.4 within the last seven years.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Part		

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~7~~8 Table R4 – ~~-~~Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP) (except for medium impact BCS without ERC).	~~An~~ Examples of evidence may include, but ~~is~~are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a ~~Physical Security Perimeter.~~PSP.
4.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated:	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account

CIP-004-~~7~~8 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
	1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part		listing), or - Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~7~~8 Table R5 – ~~-~~Access Revocation

Part	Applicable Systems	Requirements	Measures
5.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access (except for Medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated:	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts; and authorized unescorted physical access (except for Medium impact BCS without ERC) that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible

CIP-004-~~7~~8 Table R5 – ~~-~~Access Revocation

Part	Applicable Systems	Requirements	Measures
	1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	longer requires retention of that access.	Entity determines is not necessary.
5.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated EACMS SCI supporting an Applicable System in this Part.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the ~~"~~Applicable Systems~~"~~ identified in *CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1~~.)~~) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI~~.~~ (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.

CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a Medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train one individual (with the exception of CIP Exceptional Circumstances) prior	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train two individuals (with the exception of CIP Exceptional	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train three individuals (with the exception of CIP Exceptional	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. ~~(~~(Part 2.1) OR

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. ~~(~~(Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting authorized electronic or authorized unescorted	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing ~~Personnel Risk Assessments (PRAs),~~personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	access for one individual. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR	physical access for two individuals. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~through	authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the	cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal~~

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)	3.2.2 for two individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)	required checks described in 3.2.1 ~~and~~through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 ~~&~~through 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access	~~history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR ~~The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 ~~&~~through 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for four or more individuals with authorized electronic

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)	or authorized unescorted physical access within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for 5% or less of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR The Responsible Entity did not ~~implement one or more documented program(s) for access management that includes a process to~~ authorize electronic access or unescorted physical access~~. (~~ based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 5% but less than (or equal to) 10% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 10% but less than (or equal to) 15% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 15% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)
R5	The Responsible Entity ~~has implemented one or more process(es) to~~ did not revoke ~~the~~ individual's user accounts upon termination action ~~but did not do so for~~ within 30 calendar days of the date of termination action for one or more individuals. (Part 5.3) OR The Responsible Entity ~~has implemented one or more process(es) to~~did not change passwords for shared accounts known to the user upon termination action,	The Responsible Entity ~~has implemented one or more process(es) to remove the~~ did not initiate removal of the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for one individual. (Part 5.1) OR ~~The Responsible Entity has implemented one or more process(es) to determine~~	The Responsible Entity ~~has implemented one or more process(es) to remove the~~ did not initiate removal of the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for two individuals. (Part 5.1) OR	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity ~~has implemented one or more process(es) to remove~~did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action ~~but did not~~

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	reassignment, or transfer~~, but did not do so for~~ within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR ~~The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but~~The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	~~that an individual no longer requires retention of access following reassignments or transfers but,~~The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	~~The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~The Responsible Entity for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	~~initiate those removals~~ for three or more individuals. (Part 5.1) OR ~~The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~The Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity~~ has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for one individual, did not	The Responsible Entity~~ has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for two individuals, did not	The Responsible Entity~~ has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for three individuals, did	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. ~~(~~(Requirement R6) OR

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity ~~performed~~did not perform the verification required by ~~Requirement R6~~ Part 6.2 ~~more than~~within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented~~, for one ~~or more program(s) to~~individual, did not remove the individual's ability to use provisioned access to BCSI ~~but, for one individual, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity ~~performed~~did not perform the verification required by ~~Requirement R6~~ Part 6.2 ~~more than~~within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to~~, for two individuals, did remove ~~the~~each individual's ability to use provisioned access to BCSI ~~but, for two individuals, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity ~~performed~~did not perform the verification required by ~~Requirement R6~~ Part 6.2 ~~more than~~within 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to~~, for three individuals, did not remove ~~the~~each individual's ability to use provisioned access to BCSI ~~but, for three individuals, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	The Responsible Entity ~~has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity ~~performed~~did not perform the verification required by ~~Requirement R6~~ Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity ~~has implemented one~~, for four or more ~~program(s) to~~individuals, did not remove ~~the~~each individual's ability to use provisioned access to BCSI ~~but, for four or more individuals, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
8	TBD	Modified by Project 2016-02.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 Draft 5 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)
2. **Number:** CIP-005-8
3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. Generator Operator

    4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP.	Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Systems connected via a routable protocol within each ESP.
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that control an ESP for an Applicable System in Part 1.1	Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.	Examples of evidence may include, but are not limited to, documentation of the methods implemented to permit only needed network accessibility to Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the Management Interfaces (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).
1.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious routable protocol communications detection methods (e.g., intrusion detection system, application

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
			layer firewall, etc.) are implemented.
1.6	High impact BCS and their associated PCA Medium impact BCS at Control Centers and their associated PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time-sensitive communication of Protection Systems.	Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Permit Interactive Remote Access (IRA), if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	Intermediate System(s) used to access an Applicable System in Part 2.1	Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Examples of evidence may include, but are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption) initiate and terminate.
2.3	Intermediate System(s) used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Example of evidence may include, but are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID;

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			- Something the individual has such as tokens, digital certificates, or smart cards; or - Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
2.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, including IRA and system-to-system remote access, such as: - Methods for accessing logged or monitoring information to determine active vendor remote access sessions; - Methods for monitoring activity (e.g., connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g., netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or - Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High impact BCS and their associated PCA	Have one or more method(s) to	Examples of evidence may include,

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	disable active vendor remote access (including IRA and system-to-system remote access).	but are not limited to, documentation of the methods(s) used to disable active vendor remote access • (including IRA and system-to-system remote access).
2.6	Intermediate System(s) used to access an Applicable System in Part 2.1	Prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System and supporting Cyber Systems.
2.7	Intermediate System(s) used to access an Applicable System in Part 2.1	Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Network diagrams of Intermediate Systems architecture; or • Configuration, settings, or policy of the EAP which controls routable protocol communications of IRA through the ESP.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part .	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part.	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	**Violation Severity Levels**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious routable protocol communications entering or leaving the ESP required by Part 1.5. OR The Responsible Entity did not document the reason for permitting communications. (Part 1.2)	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not protect the Applicable Systems connected to the network with routable protocol with an ESP. (Part 1.1) OR The Responsible Entity did not permit only needed communications and deny all other communications, through the ESP; excluding time sensitive communications of Protection Systems. (Part 1.2) OR The Responsible Entity did not protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces for Applicable

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Systems per system capability. (Part 1.3) OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the Applicable Systems. (Part 1.4) OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to span a single ESP between PSPs, as required by Part 1.6.
R2.	The Responsible Entity does not have documented processes for one or more of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access	The Responsible Entity did not implement processes for three of the applicable Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote access

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(including IRA and system-to-system remote access) (Part 2.5).	(including IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not prevent Intermediate System(s) from sharing CPU resources or memory resources with any part of a high or medium impact BCS or associated PCAs. (Part 2.6). OR The Responsible Entity did not ensure routable protocol communications from an Intermediate System to high or medium impact BCS or associated PCAs went through an ESP (Part 2.7).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI*. (Requirement R3)	The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.1). OR	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity did not have a method to determine authenticated vendor-initiated	The Responsible Entity did not implement any processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI*. (Requirement R3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.2).	remote connections for EACMS or SCI supporting EACMS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS or SCI supporting EACMS (Part 3.2).	The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
7	11/05/2020	Adopted by the NERC Board of Trustees.	
7	03/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
7	4/5/2021	Effective Date	10/1/2022

8	TBD	Modified by Project 2016-02.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~fourth~~fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – ~~September 30~~October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	~~October 2022~~November 2023
Board adoption	~~November 2022~~December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft ~~4~~5 Definitions".

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-8

3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems”: Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP.	Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Systems connected via a routable protocol within each ESP.
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • ~~Physical isolation of an ESP;~~ • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that ~~enforce~~control an ESP for an Applicable System in Part 1.1	~~Permit~~Protect ESP and SCI configurations by implementing methods to permit only needed ~~routable protocol communications to and from~~network accessibility to Management Interfaces of Applicable Systems, ~~and deny all other routable protocol communications,~~ per system capability.	Examples of evidence may include, but are not limited to, documentation of the ~~access enforcement configuration or settings~~methods implemented to ~~or from the~~permit only needed network accessibility to Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the ~~management plane resources~~Management Interfaces (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).
1.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious ~~Internet Protocol (IP)~~routable protocol	An example of evidence may include, but is not limited to, documentation that malicious ~~Internet Protocol (IP)~~routable

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
		communications entering or leaving an ESP.	protocol communications detection methods (e.g~~.~~., intrusion detection system, application layer firewall, etc.) are implemented.
1.6	High impact BCS and their associated PCA Medium impact BCS at Control Centers and their associated PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: - Confidentiality and integrity controls, or - Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time-sensitive communication of Protection Systems.	Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: - Configurations or settings used to enforce encryption; or - The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Permit ~~authorized~~ Interactive Remote Access (IRA), if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	Intermediate ~~Systems~~System(s) used to access an Applicable System in Part 2.1	Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Examples of evidence may include, but are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption) initiate and terminate.
2.3	Intermediate System(s) used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for ~~all IRA~~IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Example of evidence may include, but are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID;

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
2.4	High impact BCS ~~with vendor remote access~~ and their associated PCA Medium impact BCS ~~with vendor remote access~~ and their associated PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, including IRA and system-to-system remote access, such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g~~.~~., connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g~~.~~., netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High impact BCS ~~with vendor remote access~~ and their associated PCA Medium impact BCS ~~with vendor remote access~~ and their associated PCA SCI supporting an Applicable System in this Part	Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access • (including IRA and system-to-system remote access).
2.6	Intermediate System(s) used to access an Applicable System in Part 2.1	Prevent Intermediate ~~Systems shall:~~ ~~2.6.1. Not share~~System(s) from sharing CPU ~~or~~resources and memory resources with any part of a high or medium impact BCS~~;~~ ~~and~~ ~~2.6.2. Restrict their routable protocol communications to BCS and their~~ or associated PCAs ~~through an ESP.~~.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System~~.~~ and supporting Cyber Systems.
2.7	Intermediate System(s) used to access an Applicable System in Part 2.1	Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Network diagrams of Intermediate Systems architecture; or • Configuration, settings, or policy of the EAP which controls routable protocol communications of IRA through the ESP.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part .	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part.	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- ~~-~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious ~~Internet Protocol (IP)~~routable protocol communications entering or leaving the ESP required by Part 1.~~6.~~ 5. OR The Responsible Entity did not document the reason for permitting communications. (Part 1.2)	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not protect the Applicable Systems connected to the network with routable protocol with an ESP. (Part 1.1) OR The Responsible Entity did not permit only needed communications ~~to and from Applicable Systems either individually or as a group~~ and deny all other communications, through the ESP; excluding time sensitive communications of Protection Systems. (Part 1.2) OR The Responsible Entity did not protect ESP and SCI configurations by implementing methods to permit only needed ~~and~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~controlled communications to and from~~network accessibility to Management Interfaces for Applicable Systems ~~and deny all other communications.~~per system capability. (Part 1.3) OR The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the Applicable Systems. (Part 1.4) OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to span a single ESP between PSPs, as required by Part 1.~~3.~~ 6. ~~OR~~ ~~The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the Applicable Systems. (Part 1.5)~~
R2.	The Responsible Entity does not have documented processes for one or more of	The Responsible Entity did not implement processes for one of the applicable Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable Requirement Parts 2.1 through 2.3;	The Responsible Entity did not implement processes for three of the applicable Requirement Parts 2.1 through 2.3;

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	the applicable Requirement Parts 2.1 through 2.3.		OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (Part 2.5).	OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote access (including IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not prevent Intermediate System(s) from sharing CPU resources or memory resources with any part of a high or medium impact BCS or associated PCAs. (Part 2.6). OR The Responsible Entity did not ensure routable protocol communications ~~are~~from an Intermediate System to high or medium impact BCS or associated PCAs went through

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				an ESP ~~as required by~~ (Part 2.~~6.~~7).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI*. (Requirement R3)	The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for EACMS or SCI supporting EACMS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS or SCI supporting EACMS (Part 3.2).	The Responsible Entity did not implement any processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI*. (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	~~TBD~~08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
7	11/05/2020	Adopted by the NERC Board of Trustees.	
7	03/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
7	4/5/2021	Effective Date	10/1/2022

8	TBD	Modified by Project 2016-02.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 5 Definitions".

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-~~7~~8

3. Purpose: To ~~manage electronic access to~~ protect BES Cyber Systems ~~by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems~~(BCS) against compromise ~~that could lead to~~ by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the ~~BES.~~Bulk Electric System (BES).

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-~~7~~8:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

~~**5. Effective Date:** See Implementation Plan for Project 2019-03.~~

~~**6. Background:** Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the~~

~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems”~~ Columns in Tables~~:

4.3. Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies.~~ The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~
- ~~**High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.~~
- ~~**High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity.~~

~~This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~

- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~
- ~~**Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

5. **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA	~~All applicable Cyber Assets~~Applicable Systems connected to a network via a routable protocol ~~shall reside within a defined~~must be protected by an ESP.	~~An example~~Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber ~~Assets~~Systems connected via a routable protocol within each ESP.
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
			configuration).
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that control an ESP for an Applicable System in Part 1.1	Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.	Examples of evidence may include, but are not limited to, documentation of the methods implemented to permit only needed network accessibility to Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the Management Interfaces (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).
1.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious routable protocol communications entering or	An example of evidence may include, but is not limited to, documentation that malicious routable protocol

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
		leaving an ESP.	communications detection methods (e.g., intrusion detection system, application layer firewall, etc.) are implemented.
1.~~2~~6	High ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS at Control Centers and their associated~~:~~ PCA	~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ~~i.~~ii. Time-sensitive communication of Protection Systems.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, ~~network diagrams showing all external routable communication paths~~documentation of methods used to protect the confidentiality and integrity of the ~~identified EAPs.~~ data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

~~CIP-005-7 Table R1 – Electronic Security Perimeter~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~1.3~~	~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	~~Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.~~	~~An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.~~
~~1.4~~	~~High Impact BES Cyber Systems with Dial-up Connectivity and their associated:~~ - ~~PCA~~ ~~Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated:~~ - ~~PCA~~	~~Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.~~	~~An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.~~
~~1.5~~	~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers~~	~~Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.~~	~~An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.~~

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, ~~where technically feasible~~per system capability, in *CIP-005-~~7~~8 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~7~~8 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS and their associated~~:~~ PCA SCI supporting an Applicable System in this Part	~~For all~~Permit Interactive Remote Access~~,~~ ~~utilize~~ (IRA), if any, only through an Intermediate System ~~such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~.	Examples of evidence may include, but are not limited to, network diagrams ~~or~~, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~Intermediate System(s) used to access an Applicable System in Part 2.1	~~For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.~~Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption ~~initiates~~) initiate and ~~terminates.~~ terminate.

CIP-005-~~7~~8 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.3	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~• PCA~~ Intermediate System(s) used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for ~~all Interactive Remote Access sessions~~IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	~~An example~~Example of evidence may include, but ~~is~~are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
2.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ ~~•~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~ impact BCS and their associated~~:~~ ~~•~~ PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, ~~(~~including ~~Interactive Remote Access~~ IRA and system-to-system remote access~~)~~, such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g., connection tables or rule hit

CIP-005-~~7~~8 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
			counters in a firewall, or user activity monitoring) or open ports (e.g., netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~ impact BCS and their associated~~:~~ PCA SCI supporting an Applicable System in this Part	Have one or more method(s) to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including ~~Interactive Remote Access~~ IRA and system-to-system remote access~~),~~ ~~such as:~~ • ~~Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or~~ • ~~Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.~~).

CIP-005-~~7~~8 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.6	Intermediate System(s) used to access an Applicable System in Part 2.1	Prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System and supporting Cyber Systems.
2.7	Intermediate System(s) used to access an Applicable System in Part 2.1	Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Network diagrams of Intermediate Systems architecture; or • Configuration, settings, or policy of the EAP which controls routable protocol communications of IRA through the ESP.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-~~7~~8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS~~SCI

Part	Applicable Systems	Requirements	Measures
3.1	EACMS and PACS associated with ~~High Impact BES Cyber Systems~~ high impact BCS. EACMS and PACS associated with ~~Medium Impact BES Cyber Systems~~medium impact BCS with ~~External Routable Connectivity~~ ERC. SCI supporting an Applicable System in this Part .	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with ~~High Impact BES Cyber Systems~~high impact BCS. EACMS and PACS associated with ~~Medium Impact BES Cyber Systems~~medium impact BCS with ~~External Routable Connectivity~~ ERC. SCI supporting an Applicable System in this Part.	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a

CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS~~SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
			firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious routable protocol communications entering or leaving the ESP required by Part 1.5. OR The Responsible Entity did not document the reason for ~~both inbound and outbound~~permitting communications. (Part 1.~~5)~~2)	The Responsible Entity did not document one or more processes for *CIP-005-~~6~~8 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not ~~have all applicable Cyber Assets~~protect the Applicable Systems connected to ~~a~~the network ~~via a~~with routable protocol ~~within a defined Electronic Security Perimeter (ESP). (~~with an ESP. (Part 1.1) OR ~~External Routable Connectivity through the ESP was not through an identified EAP. (1.2)~~ ~~OR~~ The Responsible Entity did not ~~require inbound and outbound access permissions~~permit only needed communications and deny all other

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~access~~communications, through the ESP; excluding time sensitive communications of Protection Systems. (Part 1.2) OR The Responsible Entity did not protect ESP and SCI configurations by ~~default.~~ ~~(~~implementing methods to permit only needed network accessibility to Management Interfaces for Applicable Systems per system capability. (Part 1.3) OR The Responsible Entity did not perform authentication when establishing ~~dial~~Dial-up ~~connectivity with the applicable Cyber Assets, where technically feasible.~~ ~~(~~Connectivity with the Applicable Systems. (Part 1.4) OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				span a single ESP between PSPs, as required by Part 1.6.
R2.	The Responsible Entity does not have documented processes for one or more of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5).	The Responsible Entity did not implement processes for three of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~ IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not prevent Intermediate System(s) from sharing CPU resources or memory resources with any part of

R #	**Violation Severity Levels**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				a high or medium impact BCS or associated PCAs. (Part 2.6). OR The Responsible Entity did not ensure routable protocol communications from an Intermediate System to high or medium impact BCS or associated PCAs went through an ESP (Part 2.7).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS.~~ ~~(~~SCI.* (Requirement R3)	The Responsible Entity ~~had method(s) as required by Part 3.1 for EACMS but~~ did not have a method to determine authenticated vendor-initiated remote connections for PACS ~~(~~or SCI supporting PACS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for EACMS but~~ did not have a method to terminate authenticated vendor-initiated remote connections for PACS ~~(3.2~~or SCI supporting PACS (Part 3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity ~~had method(s) as required by Part 3.1 for PACS but~~ did not have a method to determine authenticated vendor-initiated remote connections for EACMS ~~(~~or SCI supporting EACMS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for PACS but~~ did not	The Responsible Entity did not implement any processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS.~~ ~~(~~SCI.* (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS ~~(~~or SCI supporting EACMS (Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project ~~2019-03~~2016-02
- CIP-005-~~7~~8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
7	11/05/2020	Adopted by the NERC Board of Trustees.	
7	03/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
7	4/5/2021	Effective Date	10/1/2022
8	TBD	Modified by Project 2016-02.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 – September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 5 Definitions."

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002- identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See Project 2016-02 Modifications to CIP Standards Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports or network accessible logical services, individually or by group; • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; • Configuration or settings of host-based firewalls or other device level mechanisms that disable or prevent unneeded network accessible logical ports or network accessible logical services; or • Identity or process based access policy or workload configuration demonstrating needed network accessibility.

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium impact BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Examples of evidence may include, but are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting either: High impact BCS or their associated PCA. Medium impact BCS or their associated PCA.	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: - Virtualization affinity rules; or - Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Cyber Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.	Examples of evidence may include, but are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.
2.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Examples of evidence may include, but are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	this Part.		
2.3	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: - Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of component software revision, or registry exports that show software has been installed); or - A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.
2.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Examples of evidence may include, but are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of evidence may include, but are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
	this Part.		
3.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Examples of evidence may include, but are not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events, per system capability: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Control			
Part	Applicable Systems	Requirements	Measures
5.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use.
5.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify individuals who have authorized access to shared accounts.	Examples of evidence may include, but are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information:

None

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)	The Responsible Entity had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS. (Part 1.3)	The Responsible Entity neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity did not evaluate the cyber security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but	The Responsible Entity did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last	The Responsible Entity did not include any processes for installing cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R2. (Requirement R2) OR The Responsible Entity did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	less than 50 calendar days of the evaluation completion. (Part 2.3)	evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)	The Responsible Entity did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4) OR The Responsible Entity did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)
R3	N/A	The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3). OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity missed one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	The Responsible Entity missed one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity did not retain applicable security event	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity, per system capability, did not

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity missed two or more 15 calendar day intervals. (Part 4.4)	detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)
R5	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity process(es) for password-only	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity did not, per device capability, change known default passwords. (Part 5.4) OR The Responsible Entity did not technically or procedurally enforce all of the password

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			authentication for interactive user access did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity neither limited the number of unsuccessful authentication attempts nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining

Version	Date	Action	Change Tracking
			directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	TBD	Modified by Project 2016-02.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~fourth~~fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 – September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – ~~September 30~~October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	~~October 2022~~November 2023
Board adoption	~~November 2022~~December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed new or modified terms titled “Project 2016-02 Draft ~~4~~5 Definitions.”

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002- identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See Project 2016-02 Modifications to CIP Standards Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1– System Hardening

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: - Documentation of the need for all enabled network accessible logical ports or network accessible logical services, individually or by group~~.~~; - Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports;~~ or~~ - Configuration or settings of host-based firewalls or other device level mechanisms that disable or prevent unneeded network accessible logical ports or network accessible logical services~~.~~; or - Identity or process based access policy or workload configuration demonstrating needed network accessibility.

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium impact BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Examples of evidence may include, but are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting either: High impact BCS ~~and~~or their associated~~:~~ ~~• EACMS;~~ ~~• PACS; and~~ PCA. Medium impact BCS ~~and~~or their associated~~:~~ ~~• EACMS;~~ ~~• PACS; and~~ PCA.	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between ~~Virtal Cyber Assets (~~VCAs~~)~~ that are~~ not of~~, or are associated with, ~~the same~~a medium or high impact ~~categorization.~~ BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Cyber Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.	Examples of evidence may include, but are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.
2.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Examples of evidence may include, but are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Cyber Security Patch Management

Part	Applicable Systems	Requirements	Measures
	this Part.		
2.3	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; ~~or~~ - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: - Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of component software revision, or registry exports that show software has been installed); or - A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.
2.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Examples of evidence may include, but are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Prevention

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of evidence may include, but are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
	SCI supporting an Applicable System in this Part.		
3.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Examples of evidence may include, but are not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events~~(~~, per system capability~~):~~: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use.
5.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify individuals who have authorized access to shared accounts.	Examples of evidence may include, but are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: - Records of a procedure that passwords are changed when new devices are in production; or - Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: - System-generated reports or ~~screen-shots~~screenshots of the system-enforced password parameters, including length and complexity; or - Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: - System-generated reports or ~~screen-shots~~screenshots of the system-enforced periodicity of changing passwords; or - Attestations that include a reference to the documented procedures that were followed.
5.7	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: - Documentation of the account-lockout parameters; or - Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information:

None

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)	The Responsible Entity had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are~~ not of~~, or are associated with, ~~the same impact categorization.~~a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS. (Part 1.3)	The Responsible Entity neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity did not evaluate the cyber security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan	The Responsible Entity did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last	The Responsible Entity did not include any processes for installing cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R2. (Requirement R2) OR The Responsible Entity did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)	The Responsible Entity did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4) OR The Responsible Entity did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)
R3	N/A	The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3). OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity missed one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	The Responsible Entity missed one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4) OR

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity missed two or more 15 calendar day intervals. (Part 4.4)	The Responsible Entity, per system capability, did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)
R5	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity did not, per device capability, change

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			OR The Responsible Entity process(es) for password-only authentication for interactive user access did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	known default passwords. (Part 5.4) OR The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity neither limited the number of unsuccessful authentication attempts nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining

Version	Date	Action	Change Tracking
			directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	TBD	Modified by Project 2016-02.	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 – September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed new or modified terms titled "Project 2016-02 Draft 5 Definitions."

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-~~6~~7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." ~~-~~For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1 Balancing Authority

   4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~4.1.6~~4.1.5 Reliability Coordinator

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~6~~7:

4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-~~5.1~~ identification and categorization processes.

~~5. Effective Dates:~~

~~See Implementation Plan for CIP-007-6.~~

~~6. Background:~~

~~Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~” Columns in Tables:~~

4.3. ”: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies.~~ The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~

- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

5. ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~**Effective Dates:** See Project 2016-02 Modifications to CIP Standards Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R1 – ~~Ports and Services~~System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R1 – ~~Ports and Services~~System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R1– ~~Ports and Services~~System Hardening

Part	Applicable Systems	Requirements	Measures
1.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control~~Medium Impact BES Cyber~~ Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA	~~Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.~~Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports ~~on all applicable Cyber Assets and Electronic Access Points, individually~~ or ~~by group.~~network accessible logical services, individually or by group; • Listings of the listening ports ~~on the Cyber Assets~~, individually or by group, from either ~~the device~~ configuration files or settings, command output (such as netstat), or network scans of open ports; ~~or~~

CIP-007-~~6~~7 Table R1– ~~Ports and Services~~System Hardening			
Part	Applicable Systems	Requirements	Measures
	SCI supporting an Applicable System in this Part.		• Configuration ~~files~~or settings of host-based firewalls or other device level mechanisms that ~~only allow~~disable or prevent unneeded network accessible logical ports or network accessible logical services; or • Identity or process based access policy or workload configuration demonstrating needed ~~ports and deny all others.~~ network accessibility.

CIP-007-~~6~~7 Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting either: High impact BCS or their associated PCA. Medium impact BCS or their associated PCA.	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	A patch management process for tracking, evaluating, and installing cyber security patches~~ for applicable Cyber Assets~~. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for ~~applicable Cyber Assets~~Applicable Systems that are updateable and for which a patching source exists.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored~~, whether on an individual BES Cyber System or Cyber Asset basis.~~.

CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security~~-related~~ patches released by the documented sources at least once every 35 calendar days.
2.3	High ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; ~~or~~ • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of ~~BES Cyber System Component~~component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include

CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.
2.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	~~An e~~Examples of evidence may include, but ~~is~~are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Deploy method(s) to deter, detect, or prevent malicious code.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-~~6~~7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: - Records of response processes for malicious code detection - Records of the performance of these processes when malicious code is detected.
3.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation showing the process used for the update of signatures or patterns.

CIP-007-~~6~~7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
	in this Part.		

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R4 – Security Event Monitoring

Part	Applicable Systems	Requirements	Measures
4.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Log security events~~ at the BES Cyber System level (~~, per ~~BES Cyber Systems~~system capability~~) or at the Cyber Asset level (per Cyber Asset capability)~~, for identification of, and after-the-fact investigations of, Cyber Security Incidents that ~~includes, as~~include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the ~~BES Cyber~~Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber~~	Generate alerts for security events that the Responsible Entity determines necessitates an alert~~,~~ that includes, as a minimum, each of the following types of events~~ (~~, per ~~Cyber Asset or BES Cyber Systems~~system capability~~):~~: 4.2.1. Detected malicious code from Part 4.1; and	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~6~~7 Table R4 – Security Event Monitoring

Part	Applicable Systems	Requirements	Measures
	~~Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	4.2.2. Detected failure of Part 4.1 event logging.	
4.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	~~Where technically feasible, retain~~Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, ~~any~~ findings from the review (if any), and dated documentation showing the review occurred.

CIP-007-~~6~~7 Table R4 – Security Event Monitoring			
Part	Applicable Systems	Requirements	Measures
	in this Part.		

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Have a method(s) to enforce authentication of interactive user access, ~~where technically feasible~~per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~6~~7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use.
5.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify individuals who have authorized access to shared accounts.	Examples of evidence may include, but are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~6~~7 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~7 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.6	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

~~CIP-007-6 Table R5 – System Access Control~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~5.2~~	~~High Impact BES Cyber Systems and their associated:~~ ~~4. EACMS;~~ ~~5. PACS; and~~ ~~6. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).~~	~~An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.~~

~~CIP-007-6 Table R5 – System Access Control~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~5.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Identify individuals who have authorized access to shared accounts.~~	~~An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.~~

~~CIP-007-6 Table R5 – System Access Control~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~5.4~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Change known default passwords, per Cyber Asset capability~~	~~Examples of evidence may include, but are not limited to:~~ ~~• Records of a procedure that passwords are changed when new devices are in production; or~~ ~~• Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.~~

~~CIP-007-6 Table R5 – System Access Control~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~5.5~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:~~ ~~5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and~~ ~~5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or~~ ~~• Attestations that include a reference to the documented procedures that were followed.~~

~~CIP-007-6 Table R5 – System Access Control~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~5.6~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or~~ ~~• Attestations that include a reference to the documented procedures that were followed.~~

~~CIP-007-6 Table R5 – System Access Control~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
~~5.7~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems at Control Centers and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Where technically feasible, either:~~ • ~~Limit the number of unsuccessful authentication attempts; or~~ • ~~Generate alerts after a threshold of unsuccessful authentication attempts.~~	~~Examples of evidence may include, but are not limited to:~~ • ~~Documentation of the account-lockout parameters; or~~ • ~~Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.~~

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information:

None

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	~~R1~~The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)	The Responsible Entity ~~has implemented and documented processes for Ports and Services but~~ had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity ~~has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,~~ had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS. (Part 1.3)	The Responsible Entity ~~did not implement or document~~neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security~~	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~7 Table R2. (Requirement R2)

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~patches for applicability but~~ did not evaluate the cyber security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	include any processes, including the identification of sources, for tracking or evaluating cyber security patches for ~~applicable Cyber Assets. (~~Applicable Systems. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~	include any processes for installing cyber security patches for ~~applicable Cyber Assets. (~~Applicable Systems. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan	OR The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but~~ did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch but~~ did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	within 65 calendar days of the evaluation completion. (Part 2.3)	
R3	N/A	The Responsible Entity ~~has implemented one or more documented process(es), but~~, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention, but~~, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3). OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	The Responsible Entity ~~has documented and implemented~~ missed one ~~or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling~~ of ~~logged events at least every~~ 15 calendar ~~days but missed an~~day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	The Responsible Entity ~~has documented and implemented~~ missed one ~~or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every~~ 15 calendar ~~days but missed an~~day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity ~~has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but~~ did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity ~~has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but~~ did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity ~~has documented and~~	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity ~~has documented and implemented one or more process(es) to log events for the Applicable Systems (~~, per ~~device or~~ system capability~~)~~ ~~but~~, did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but~~ missed two or more 15 calendar day intervals. (Part 4.4)	
R5	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification of the individuals	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity ~~has implemented one or more~~

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented~~ process(es) for password-only authentication for interactive user access ~~that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for~~	~~documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but~~ did not, per device capability, change known default passwords. (Part 5.4) OR ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the~~The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit~~neither limited the number of unsuccessful authentication attempts ~~or generate~~nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining

Version	Date	Action	Change Tracking
			directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.~~

~~**1.1.** This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'~~

~~**1.2.** Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.~~

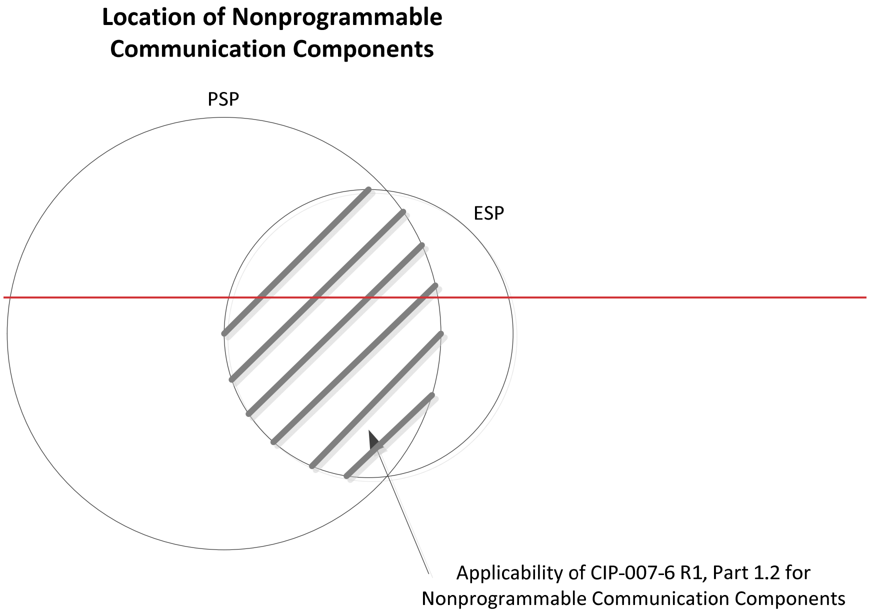
~~The protection of these ports can be accomplished in several ways including, but not limited to:~~

- ~~Disabling all unneeded physical ports within the Cyber Asset's configuration~~
- ~~Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization~~
- ~~Physical port obstruction through removable locks~~

~~The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.~~

~~This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.~~

~~The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:~~



~~**Requirement R2:**~~

~~The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.~~

~~Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.~~

~~One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.~~

~~**2.1.** The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they~~

~~can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.~~

~~**2.2.** Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.~~

~~When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.~~

~~**2.3.** The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or~~

~~those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.~~

~~**2.4.** The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.~~

~~**Requirement R3:**~~

~~**3.1.** Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.~~

~~**3.2.** When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or~~

~~method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.~~

~~Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media (“transient devices”) in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.~~

~~**3.3.** In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System’s ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a ‘false positive’ could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.~~

~~**Requirement R4:**~~

~~Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.~~

~~**4.1.** In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.~~

~~Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.~~

~~User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.~~

~~It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.~~

~~**4.2.** Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.~~

~~The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:~~

- ~~Detected known or potential malware or malicious activity~~
- ~~Failure of security event logging mechanisms~~
- ~~Login failures for critical accounts~~
- ~~Interactive login of system accounts~~
- ~~Enabling of accounts~~
- ~~Newly provisioned accounts~~
- ~~System administration or change tasks by an unauthorized user~~
- ~~Authentication attempts on certain accounts during non-business hours~~
- ~~Unauthorized configuration changes~~
- ~~Insertion of Removable Media in violation of a policy~~

~~**4.3** Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.~~

~~**4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-~~

~~time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.~~

~~**Requirement R5:**~~

~~Account types referenced in this guidance typically include:~~

- ~~Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.~~
- ~~Individual user account: An account used by a single user.~~
- ~~Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.~~
- ~~System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.~~
- ~~Application account: A specific system account, with rights granted at the application level often used for access into a Database.~~
- ~~Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.~~
- ~~Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.~~
- ~~Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.~~

~~**5.1** Reference the Requirement's rationale.~~

~~**5.2** Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.~~

~~**5.3** Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.~~

~~**5.4.** Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.~~

~~The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.~~

~~**5.5.** Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.~~

~~Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.~~

~~**5.6** Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.~~

~~**5.7** Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.~~

~~Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.~~

~~In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.~~

~~The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).~~

~~Rationale for Requirement R2:~~

~~Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.~~

~~Rationale for Requirement R3:~~

~~Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.~~

~~Rationale for Requirement R4:~~

~~Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.~~

~~Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.~~

~~Rationale for Requirement R5:~~

~~To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.~~

~~Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.~~

~~Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.~~

~~Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.~~

~~For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.~~

~~The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.~~

~~The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.~~

~~The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.~~

~~Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting~~	TBD	Modified by Project 2016-02.	

~~the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.~~7			

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed of modified terms titled “Project 2016-02 Draft 5 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and

data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.	Examples of evidence may include, but are not limited to, one or more documented process(es) that authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity, such as: • Change records documenting the authorization. • Change records authorizing systems to automate changes to Applicable Systems. Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software,

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) • Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) • Configuration of malicious code prevention methods (CIP-007 R3) • Configuration of security event logging/alerting (CIP-007 R4) • Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5) • Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)
1.2	High impact BCS	1.2.1. Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, to ensure that required cyber security controls in CIP-005 and CIP-	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test, or logs from systems that automatically remediate deviations in required cyber security controls in CIP-005 and CIP-007.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		007 are not adversely affected; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.
1.4	High impact BCS and their associated: 1. EACMS;	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the	An example of evidence may include, but is not limited to:

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	altered cyber security controls were not adversely affected.	• System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods;	An example of evidence may include, but is not limited to, documented methods to monitor at least once every 35 calendar days. Monitoring system configuration or procedural controls demonstrating monitoring of at least one cyber security control for 2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	Applicable Systems	Requirements	Measures
		2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements or additions with a previously assessed configuration of an existing Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of tools used to perform the assessment; or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of evidence may include, but are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA, and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.		The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity change management process(es) did not include authorization for changes as required in Part 1.1. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. (Part 1.2); OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) OR The Responsible Entity's change management process(es) does not include verification, as required by Part 1.4. (Part 1.4)	The Responsible Entity neither documented nor implemented any change management process(es) that include required items in Part 1.1 through Part 1.4. (Requirement R1)
R2.	The Responsible Entity did not monitor within 35 calendar	The Responsible Entity's documented and implemented	The Responsible Entity's documented and implemented	The Responsible Entity neither documented nor implemented

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	days, but less than 70 calendar days as required by Part 2.1.	configuration monitoring process(es) does not include one or two of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 70 calendar days, but less than 105 calendar days as required by Part 2.1.	configuration monitoring process(es) does not include three or four of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 105 calendar days, but less than 140 calendar days as required by Part 2.1.	a configuration monitoring process(es); or the process does not include five or more of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 140 calendar days or more as required by Part 2.1. OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1)
R3.	The Responsible Entity performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more	The Responsible Entity performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more	The Responsible Entity performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more	The Responsible Entity did not implement any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3) OR The Responsible Entity performed a vulnerability assessment more than 24 months since the last assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	than 36 months, but less than 39 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	than 39 months, but less than 42 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	than 42 months, but less than 45 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2) OR The Responsible Entity did not perform the active vulnerability assessment of a Cyber System prior to it becoming an Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)
R4.	The Responsible Entity did not manage its Transient Cyber Asset(s) according to Attachment 1, Section 1.1. (Requirement R4) OR The Responsible Entity did not document the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document authorization for TCA managed by the Responsible Entity according to Attachment 1, Section 1.2. (Requirement R4)	The Responsible Entity did not implement the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCA managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the	The Responsible Entity did not authorize its TCA(s) according to Attachment 1, Section 1.2. (R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to Attachment 1,	The Responsible Entity did not document or implement one or more plan(s) for TCAs and Removable Media according to Requirement R4. (Requirement R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.
- CIP-010-5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	
5	TBD	Modified by Project 2016-02.	

Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Live operating system and software executable only from read only media;
- System hardening; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or

- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read only media;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

2.3. For any method used as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCA(s). This can be included as part of the TCA(s), part of the documentation related to authorization of TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating system and software executable only from read only media, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the risk of software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, methods to maintain the known good state of the OS and all software, or system hardening practices. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that that document a review of the use of live operating system and software executable only from read only media;

memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that that document a review of the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, and system hardening by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed of modified terms titled “Project 2016-02 Draft 5 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and

data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.	Examples of evidence may include, but are not limited to, one or more documented process(es) that authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity, such as: • Change records documenting the authorization. • Change records authorizing systems to automate changes to Applicable Systems. Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software,

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2) - Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) - Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) - Configuration of malicious code prevention methods (CIP-007 R3) - Configuration of security event logging/alerting (CIP-007 R4) - Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5) - Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)
1.2	High impact BCS	1.2.1. Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, to ensure that required cyber security controls in CIP-005 and CIP-	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test, or logs from systems that automatically remediate deviations in required cyber security controls in CIP-005 and CIP-007.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		007 are not adversely affected; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.
1.4	High impact BCS and their associated: 1. EACMS;	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the	An example of evidence may include, but is not limited to:

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	altered cyber security controls were not adversely affected.	• System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods;	An example of evidence may include, but is not limited to, documented methods to monitor at least once every 35 calendar days. Monitoring system configuration or procedural controls demonstrating monitoring of at least one cyber security control for 2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
		2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements or additions with a previously assessed configuration of an existing Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of tools used to perform the assessment; or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of evidence may include, but are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA, and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.		The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity change management process(es) did not include authorization for changes as required in Part 1.1. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. (Part 1.2); OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) OR The Responsible Entity's change management process(es) does not include verification, as required by Part 1.4. (Part 1.4)	The Responsible Entity neither documented nor implemented any change management process(es) that include required items in Part 1.1 through Part 1.4. (Requirement R1)
R2.	The Responsible Entity did not monitor within 35 calendar	The Responsible Entity's documented and implemented	The Responsible Entity's documented and implemented	The Responsible Entity neither documented nor implemented

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	days, but less than 70 calendar days as required by Part 2.1.	configuration monitoring process(es) does not include one or two of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 70 calendar days, but less than 105 calendar days as required by Part 2.1.	configuration monitoring process(es) does not include three or four of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 105 calendar days, but less than 140 calendar days as required by Part 2.1.	a configuration monitoring process(es); or the process does not include five or more of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 140 calendar days or more as required by Part 2.1. OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1)
R3.	The Responsible Entity performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more	The Responsible Entity performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more	The Responsible Entity performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more	The Responsible Entity did not implement any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3) OR The Responsible Entity performed a vulnerability assessment more than 24 months since the last assessment on one of its

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>than 36 months, but less than 39 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)</td><td>than 39 months, but less than 42 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)</td><td>than 42 months, but less than 45 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)</td><td>applicable BES Cyber Systems. (Part 3.1)
OR
The Responsible Entity performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2)
OR
The Responsible Entity did not perform the active vulnerability assessment of a Cyber System prior to it becoming an Applicable Systems. (Part 3.3)
OR
The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date</td></tr>
</table>

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td></td><td>of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)</td></tr>
<tr><td>R4.</td><td>The Responsible Entity did not manage its Transient Cyber Asset(s) according to Attachment 1, Section 1.1. (Requirement R4)
OR
The Responsible Entity did not document the Removable Media sections according to Attachment 1, Section 3. (Requirement R4)
OR
The Responsible Entity did not document authorization for TCA managed by the Responsible Entity according to Attachment 1, Section 1.2. (Requirement R4)</td><td>The Responsible Entity did not implement the Removable Media sections according to Attachment 1, Section 3. (Requirement R4)
OR
The Responsible Entity did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCA managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4)
OR
The Responsible Entity did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the</td><td>The Responsible Entity did not authorize its TCA(s) according to Attachment 1, Section 1.2. (R4)
OR
The Responsible Entity did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4)
OR
The Responsible Entity did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to Attachment 1,</td><td>The Responsible Entity did not document or implement one or more plan(s) for TCAs and Removable Media according to Requirement R4. (Requirement R4)</td></tr>
</table>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.
- CIP-010-5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	
5	TBD	Modified by Project 2016-02.	

Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- ~~Live operating system and software executable only from read only media;~~
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Live operating system and software executable only from read only media;
- System hardening; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;

- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- ~~Review use of live operating system and software executable only from read only media;~~
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read only media;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

2.3. For any method used as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCA(s). This can be included as part of the TCA(s), part of the documentation related to authorization of TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating system and software executable only from read only media, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the risk of software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, methods to maintain the known good state of the OS and all software, or system hardening practices. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that that document a review of the use of live operating system and software executable only from read only media; memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that that document a review of the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, and system hardening by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~fourth~~fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – ~~September 30~~October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	~~October 2022~~November 2023
Board adoption	~~November 2022~~December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed of modified terms titled “Project 2016-02 Draft ~~4~~5 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

~~1.~~2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

~~2.~~4. **Applicability:**

~~2.1.~~4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

~~2.2.~~4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

~~3.~~**5.** **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to ~~manages~~manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 –~~ Security~~ Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – ~~Security~~ Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – ~~Security~~ Configuration Change Management

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated: 1. Electronic Access Control ~~and~~or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	~~Control~~Authorize changes that affect Applicable Systems where those changes alter the ~~implementation~~behavior of ~~intended changes to software,~~one or ~~intended changes to settings that could weaken configured~~more cyber security controls~~ required by ~~, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 ~~and~~or CIP-007~~.~~ ~~For those changes:~~ ~~1.1.1. Authorize ~~, as defined by the ~~changes; and~~ ~~1.1.2. Verify the required cyber security controls remain implemented as required as a part of the change.~~ ~~Changes to software include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches.~~ Responsible Entity.	Examples of evidence may include, but are not limited to, ~~a~~one or more documented process(es) that ~~controls intended~~authorize changes ~~to settings that may weaken~~that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 ~~and~~or CIP-007, ~~such ~~as~~:~~ ~~• Operating system (OS) software;~~ ~~• Firmware;~~ ~~• Commercially available or open-source application software, including application containers;~~ ~~• Custom software installed, including application containers;~~ ~~• Configuration that modifies network accessible logical ports or network accessible services on an Applicable System;~~ ~~• SCI configuration of host affinity control between systems with different~~

CIP-010-5 Table R1 – ~~Security~~ Configuration Change Management

Part	Applicable Systems	Requirements	Measures
			~~impact ratings;~~ ~~• Changes to configurations or settings for an ESP between systems with different impact ratings;~~ ~~• Changes to parent images from which individual child images are derived, such as in virtual desktop infrastructure (VDI) implementations; or~~ ~~Any other configuration or setting determined~~ defined by the Responsible Entity~~.~~, such as: ~~(1.1.1.)~~ • ~~A change request record and associated~~Change records documenting the authorization ~~for applicable changes; or~~. ~~•~~ ~~Records from a change management system that identifies applicable~~Change records authorizing systems to automate changes ~~and records~~to Applicable Systems. ~~•~~ Examples of ~~authorization for~~ changes~~.~~ ~~(1.1.2.)~~ ~~A list~~ that may alter the behavior of one or more cyber security controls ~~verified along with the dated results;~~may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software,

CIP-010-5 Table R1 – ~~Security~~ Configuration Change Management

Part	Applicable Systems	Requirements	Measures
			or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • ~~A dated output from cyber~~Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) • Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) • Configuration of malicious code prevention methods (CIP-007 R3) • Configuration of security ~~tools such as~~event logging/alerting (CIP-007 R4) • Configuration changes to authentication methods (e.g., a ~~vulnerability scanner.~~password enforcement policy change, but not users changing their password) (CIP-007 R5) • Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)
1.2	High impact BCS	1.2.1. Prior to implementing ~~an intended~~any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test~~.~~ , or logs from systems that automatically

CIP-010-5 Table R1 – ~~Security~~ Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		minimizes adverse effects, to ensure that ~~the configuration of~~ required cyber security controls in CIP-005 and CIP-007 ~~remain implemented as required~~are not adversely affected; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	remediate deviations in required cyber security controls in CIP-005 and CIP-007.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and	Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

CIP-010-5 Table R1 – ~~Security~~ Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	(2) vendor performance and adherence to a contract.		
1.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the altered cyber security controls were not adversely affected.	An example of evidence may include, but is not limited to: • System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – ~~Security~~ Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – ~~Security~~ Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – ~~Security~~ Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes ~~to software, or unauthorized~~that affect Applicable Systems, where those changes ~~to settings that could weaken configured~~alter the behavior of one or more cyber security controls~~ required by CIP-005~~, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, ~~per system capability.~~ as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.	An example of evidence may include, but is not limited to, ~~logs or records from a~~documented methods to monitor at least once every 35 calendar days. Monitoring system ~~that is~~ configuration or procedural controls demonstrating monitoring of at least one cyber security control for ~~unauthorized changes~~2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

CIP-010-5 Table R2 – ~~Security~~ Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
		2.1.4. Configuration of malicious code protection methods; 2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every -15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.2	High impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements ~~of the same type of Cyber System~~or additions with a previously assessed configuration of ~~the previous or other~~an existing ~~Cyber~~Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of ~~any~~ tools used to perform the assessment~~,~~; or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of evidence may include, but are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA, and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority:** “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.		~~The Responsible Entity's change management process(es) does not include two of the required items listed in 1.1.1 through 1.1.3. (Part 1.1);~~ ~~OR~~ The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity change management ~~-~~process(es) did not include ~~the three~~authorization for changes as required ~~items listed~~ in Part 1.1.~~1 through 1.1.3.~~ (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. ~~-~~(Part 1.2); OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) OR The Responsible Entity's change management process(es) does not include verification, as required by Part 1.4. (Part 1.4)	The Responsible Entity neither documented nor implemented any change management process(es) that include required items in Part 1.1 through Part 1.~~2~~4. (Requirement R1)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.	~~N/A~~The Responsible Entity did not monitor within 35 calendar days, but less than 70 calendar days as required by Part 2.1.	~~N/A~~The Responsible Entity's documented and implemented configuration monitoring process(es) does not include one or two of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 70 calendar days, but less than 105 calendar days as required by Part 2.1.	The Responsible Entity's documented and implemented configuration monitoring process(es) does not include three or four of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not ~~document nor implemented a process(es) with methods to~~ monitor ~~for unauthorized changes at least once every 35~~within 105 calendar days~~.~~ ~~(Part 2.1);~~ ~~OR~~ ~~The Responsible Entity neither documented nor investigated detected unauthorized changes. (~~, but less than 140 calendar days as required by Part 2.1~~);~~.	The Responsible Entity neither documented nor implemented a configuration monitoring process(es~~) with methods to~~); or the process does not include five or more of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor ~~for, i at least once every 35~~within 140 calendar days ~~and~~or more as required by Part 2.1. OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1)
R3.	The Responsible Entity performed a vulnerability assessment more than 15 months, but less than 18	The Responsible Entity performed a vulnerability assessment more than 18 months, but less than 21	The Responsible Entity performed a vulnerability assessment more than 21 months, but less than 24	The Responsible Entity did not implement any vulnerability assessment processes for one

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	of its Applicable Systems. (Requirement R3) OR The Responsible Entity performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2) OR The Responsible Entity did not perform the active vulnerability assessment of a Cyber System prior to it becoming an Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				documented vulnerability assessment processes for each of its Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)
R4.	The Responsible Entity did not manage its Transient Cyber Asset(s) according to Attachment 1, Section 1.1. (Requirement R4) OR The Responsible Entity did not document the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document authorization for TCA managed by the Responsible Entity according to	The Responsible Entity did not implement the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCA managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4)	The Responsible Entity did not authorize its TCA(s) according to Attachment 1, Section 1.2. (R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4)	The Responsible Entity did not document or implement one or more plan(s) for TCAs and Removable Media according to Requirement R4. (Requirement R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Attachment 1, Section 1.2. (Requirement R4)	OR The Responsible Entity did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1~~.3,~~ ~~1.4~~, 2.2, and ~~1.5~~2.3. (Requirement R4)	OR The Responsible Entity did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.
- CIP-010-5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. -Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	

~~CIP-010-4~~ 5	TBD	Modified by Project 2016-02.	

Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- ~~Controls that maintain the state of theLive operating system and software such that it is in a known state prior to executionexecutable only from read only media;~~
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- ~~Controls that maintain the state of the operating system and software such that it is in a known state prior to execution;~~
- Live operating system and software executable only from read only media;
- Application whitelisting;
- System hardening; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review use of live operating system and software executable only from read only media;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- ~~Review of controls that maintain the state of the operating system and software such that it is in a known state prior to execution that mitigates the risk of introduction of malicious code;~~
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

2.3. For any method used~~ to mitigate software vulnerabilities or malicious code~~ as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-~~4~~5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCA(s). This can be included as part of the TCA(s), part of the documentation related to authorization of TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating system and software executable only from read only media, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the risk of software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, methods to maintain the known good state of the OS and all software, or system hardening practices. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, ~~controls to maintain the known good state of the OS and all software~~processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that that document a review of the use of live operating system and software executable only from read only media; memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that that document a review of the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, ~~controls to maintain the known good state of the OS and all software~~and system hardening by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the fifth draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21–March 22, 2021
63-day formal comment period with additional ballot	June 30 –September 1, 2021
53-day formal comment period with additional ballot	February 18 – April 12, 2022
45-day formal comment period with additional ballot	August 17 – October 3, 2022

Anticipated Actions	Date
45-day formal comment period with additional ballot	October – November 2023
Final Ballot	November 2023
Board adoption	December 2023

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed of modified terms titled “Project 2016-02 Draft 5 Definitions”.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

~~1.~~2. **Number:** CIP-010-~~4~~5

Purpose: To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting ~~BES Cyber Systems~~BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

~~2.~~3. **Applicability:**

~~2.1.~~3.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

~~2.2.~~3.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-~~4~~5:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic

Security Perimeters~~.~~ (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.5.**~~**4.2.3.6.** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

~~**3.** **Effective Date:** See Implementation Plan for Project 2019-03.~~

~~**4.** **Background:** Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be~~

~~referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~” Columns in Tables:~~

4.3. ”: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies.~~ The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples~~

~~may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

4. Effective Date: See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-~~4~~5 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~4~~5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~4~~5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~**1.1**~~	~~High Impact BES Cyber Systems and their associated:~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Develop a baseline configuration, individually or by group, which shall include the following items:~~ ~~1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;~~ ~~1.1.2. Any commercially available or open-source application software (including version) intentionally installed;~~ ~~1.1.3. Any custom software installed;~~ ~~1.1.4. Any logical network accessible ports; and~~ ~~1.1.5. Any security patches applied.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or~~ ~~• A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.~~
~~**1.2**~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~	~~Authorize and document changes that deviate from the existing baseline configuration.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• A change request record and~~

CIP-010-~~4~~5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~		~~associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or~~ ~~• Documentation that the change was performed in accordance with the requirement.~~
~~1.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.~~	~~An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.~~
1.~~4~~1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control~~Medium Impact BES Cyber~~ Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated:	~~For a change~~Authorize changes that ~~deviates from~~affect Applicable Systems where those changes alter the ~~existing baseline configuration:~~ ~~1.4.1. Prior to the change, determine required~~behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, ~~a list~~one or more documented process(es) that authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls ~~verified or tested along with the dated test results.~~, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as

CIP-010-~~4~~5 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	~~4.~~1. EACMS; ~~5.~~2. PACS; and ~~6.~~3. PCA SCI supporting an Applicable System in this Part.	parts in CIP-005 ~~and~~or CIP-007 ~~that could be impacted~~, as defined by the ~~change;~~ ~~1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and~~ ~~Document the results of the verification~~Responsible Entity.	defined by the Responsible Entity, such as: • Change records documenting the authorization. • Change records authorizing systems to automate changes to Applicable Systems. Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) • Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) • Configuration of malicious code prevention methods (CIP-007 R3) • Configuration of security event logging/alerting (CIP-007 R4) • Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5)

CIP-010-~~4~~5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			- Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)
1.~~5~~2	High ~~Impact BES Cyber Systems~~impact BCS	~~Where technically feasible, for each change that deviates from the existing baseline configuration:~~ 1.2.1. Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, ~~that models the baseline configuration~~ to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test~~.~~ , or logs from systems that automatically remediate deviations in required cyber security controls in CIP-005 and CIP-007.
1.~~6~~3	High ~~Impact BES Cyber Systems~~impact BCS and their associated:	Prior to ~~a change that deviates from~~ the ~~existing baseline configuration~~	An example of evidence may include, but is not limited to a change request record that

CIP-010-~~4~~5 Table R1 – ~~-~~Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	~~associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5,~~installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.~~6~~3.1.~~-~~ Verify the identity of the software source; and 1.~~6~~3.2.~~-~~ Verify the integrity of the software obtained from the software source.	demonstrates the verification of identity of the software source and integrity of the software was performed prior to ~~the baseline change~~installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.
1.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the altered cyber security controls were not adversely affected.	An example of evidence may include, but is not limited to: • System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-~~4~~5 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~4~~5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~4~~5 Table R2 – ~~-~~Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	~~Monitor~~Methods to monitor, per system capability, at least once every 35 calendar days, for ~~changes to~~ unauthorized changes that affect Applicable Systems, where those changes alter the ~~baseline configuration (as described~~behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in ~~Requirement R1, Part~~ CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1~~).~~ . Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.	An example of evidence may include, but is not limited to, ~~logs from a~~documented methods to monitor at least once every 35 calendar days. Monitoring system ~~that is monitoring the~~ configuration or procedural controls demonstrating monitoring of at least one cyber security control for 2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

CIP-010-45 Table R2 – -Configuration Monitoring

Part	Applicable Systems	Requirements	Measures
		2.1.4. Configuration of malicious code protection methods; 2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~3~~5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~4~~5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.1	High ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every ~~-~~15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-~~4~~5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.2	High ~~I~~impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	~~Where technically feasible, at~~At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects~~, that models the baseline configuration of the BES Cyber System in a production environment~~; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~4~~5 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Prior to ~~adding~~becoming a new ~~applicable Cyber Asset to a production environment~~Applicable System, perform an active vulnerability assessment of the new ~~Cyber Asset~~Applicable System, except for ~~CIP Exceptional Circumstances and like~~: • Like replacements ~~of the same type of Cyber Asset~~or additions with a ~~baseline~~previously assessed configuration ~~that models~~of an existing ~~baseline configuration of the previous or other existing Cyber Asset.~~Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to~~, a document listing~~: • The output of tools used to perform the assessment; or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment ~~(~~performed prior to ~~the commissioning of the~~ becoming a new ~~Cyber Asset) and the output of any tools used to perform the assessment.~~ Applicable System.

CIP-010-~~4~~5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to~~, a document~~: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA, and associated ~~Protected Cyber Assets~~SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for ~~Transient Cyber Assets~~TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for ~~Transient Cyber Assets~~TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use ~~Transient Cyber Asset~~TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use ~~Transient Cyber Asset~~TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)~~	The Responsible ~~Entity has documented and implemented a configuration~~Entity's change management process(es) ~~that includes only three~~does not include one of the required ~~baseline~~ items listed in 1.~~1~~2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.~~5. (~~3.1~~.~~ through 1.3.2. (Part 1.3)	The Responsible Entity ~~has documented and implemented a configuration~~ change management process(es) ~~that includes only two of the~~ did not include authorization for changes as required ~~baseline~~in Part 1.1. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.~~1~~2.1 through 1.2.2. (Part 1.~~5. (1.1)~~2); OR The Responsible ~~Entity has a~~Entity's change management process~~as specified in Part 1.6 to verify the identity of the software source (1.6.1) but~~(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) OR	The Responsible Entity ~~has not~~neither documented ~~or~~nor implemented any ~~configuration change management process(es). (R1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration~~ change management process(es) that ~~includes only one of the~~include required ~~baseline~~ items ~~listed~~ in Part 1.~~1.~~1 through ~~1.1.5. (1.1)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2~~Part ~~)~~ ~~OR~~

R #	**Violation Severity Levels**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
			~~have a~~The Responsible Entity's change management process~~ as specified in ~~(es) does not include verification, as required by Part 1.~~6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2~~4. (Part 1.4)	~~The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (~~1.4.~~1~~ (Requirement R1) ~~OR~~ ~~The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)~~ ~~OR~~ ~~The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1)~~ ~~OR~~ ~~The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)~~ ~~OR~~ ~~The Responsible Entity does not have a process as specified in Part 1.6 to verify~~

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td></td><td>~~the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)~~</td></tr>
<tr><td>R2.</td><td>~~N/A~~The Responsible Entity did not monitor within 35 calendar days, but less than 70 calendar days as required by Part 2.1.</td><td>~~N/A~~The Responsible Entity’s documented and implemented configuration monitoring process(es) does not include one or two of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1.
OR
The Responsible Entity did not monitor within 70 calendar days, but less than 105 calendar days as required by Part 2.1.</td><td>~~N/A~~The Responsible Entity’s documented and implemented configuration monitoring process(es) does not include three or four of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1.
OR
The Responsible Entity did not monitor within 105 calendar days, but less than 140 calendar days as required by Part 2.1.</td><td>The Responsible Entity ~~has not~~neither documented ~~or~~nor implemented a configuration monitoring process(es~~) to~~); or the process does not include five or more of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1.
OR
The Responsible Entity did not monitor ~~for, investigate, and document~~within 140 calendar days or more as required by Part 2.1.
OR
The Responsible Entity neither documented nor investigated detected unauthorized changes~~ to the baseline at~~</td></tr>
</table>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~least once every 35 calendar days. (~~. (Part 2.1)
R3.	The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its ~~applicable BES~~	The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its ~~applicable BES~~	The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its ~~applicable BES~~	The Responsible Entity ~~has~~did not ~~implemented~~implement any vulnerability assessment processes for one of its ~~applicable BES Cyber~~Applicable Systems. (Requirement R3) OR The Responsible Entity ~~has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity ~~has implemented one or more documented active vulnerability assessment processes for Applicable~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Cyber~~Applicable Systems. (Part 3.2)	~~Cyber~~Applicable Systems. (Part 3.2)	~~Cyber~~Applicable Systems. (Part 3.2)	~~Systems, but has~~ performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems~~.(~~. (Part 3.2) OR The Responsible Entity ~~has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but~~ did not perform the active vulnerability assessment ~~in~~of a ~~manner that models~~Cyber System prior to it becoming an ~~existing baseline configuration of its applicable BES Cyber~~Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				of its ~~applicable BES Cyber~~Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)
R4.	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not manage its Transient Cyber Asset(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.1. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document the Removable Media sections	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement the Removable Media sections according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to~~did not document mitigation of software vulnerabilities, mitigation for	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not authorize its ~~Transient Cyber Asset~~TCA(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement mitigation of software vulnerabilities, mitigation for	The Responsible Entity ~~failed to~~did not document or implement one or more plan(s) for ~~Transient Cyber Assets~~TCAs and Removable Media according to ~~CIP-010-4,~~ Requirement R4. (Requirement R4)

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document authorization for ~~Transient Cyber Assets~~TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (Requirement R4)	the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCAs managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for ~~Transient Cyber Assets~~TCAs managed by a party other than the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan~~ for Project 2019-03.~~”.
- CIP-010-45 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. -Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	
5	TBD	Modified by Project 2016-02.	

~~CIP-010-4 -~~ Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. ~~Transient Cyber Asset~~TCA(s) Managed by the Responsible Entity.

1.1. ~~Transient Cyber Asset~~TCA Management: Responsible Entities shall manage ~~Transient Cyber Asset~~TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection ~~to a BES Cyber System~~, or (3) a combination of both (1) and (2) above.

1.2. ~~Transient Cyber Asset~~TCA Authorization: For each individual or group of ~~Transient Cyber Asset~~TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset (per Transient Cyber Asset~~TCA (per TCA capability):

- Security patching, including manual or managed updates;
- ~~Live operating system and software executable only from read-only media;~~
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; ~~or~~
- Live operating system and software executable only from read only media;
- System hardening; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of ~~Transient Cyber Asset~~TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. ~~Transient Cyber Asset~~TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset (per Transient Cyber Asset~~TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review use of live operating system and software executable only from read only media;
- Review of other vulnerability mitigation performed by the party; or
- ~~Other~~Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- ~~Review use of live operating system and software executable only from read-only media;~~
- Review of system hardening used by the party; or
- ~~Other~~Review of other method(s) to mitigate the risk of introduction of malicious code.

2.3. For any method used ~~to mitigate software vulnerabilities or malicious code~~ as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset~~TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code~~ to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets~~, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media ~~using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets~~prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code~~ on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets~~.

CIP-010-~~4~~5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the ~~Transient Cyber Asset~~TCA(s). This can be included as part of the ~~Transient Cyber Asset plan~~TCA(s), part of the documentation related to authorization of ~~Transient Cyber Asset~~TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of ~~Transient Cyber Asset~~TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating ~~systems~~ system and software executable only from read~~-~~only media, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the risk of software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, methods to maintain the known good state of the OS and all software, or ~~procedures or processes associated with~~ system hardening practices. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail,

policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that that document a review of the use of live operating system and software executable only from read only media; memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that that document a review of the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, ~~use of live of operating systems or~~and system hardening ~~performed~~ by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2016-02 Modifications to CIP Standards Implementation Plan

Applicable Standard(s)

- Reliability Standard CIP-002-7 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-10 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-8 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-8 – Cyber Security – BES Cyber System Logical Isolation
- Reliability Standard CIP-006-7 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-7 – Cyber Security – System Security Management
- Reliability Standard CIP-008-7 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-5 – Cyber Security – Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-4 – Cyber Security – Information Protection
- Reliability Standard CIP-013-3 – Cyber Security – Supply Chain Risk Management
- Proposed new or modified terms listed in the “CIP Definitions Project 2016-02 Modifications to CIP Standards Draft 5”.

  These standards and Definitions of Terms used in the versions listed above of the CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

  These standards and new and modified terms used in the standards above will be referenced as the “Revised CIP Standards and Definitions” within the Implementation Plan.

Requested Retirement(s)

- Reliability Standard CIP-002-5.1a – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-9 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-7 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)
- Reliability Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-6 – Cyber Security – System Security Management

- Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-3 – Cyber Security – Information Protection
- Reliability Standard CIP-013-2 – Cyber Security – Supply Chain Risk Management

These standards and definitions used in the versions listed above will be referenced as the "Requested CIP Retired Standards" within the Implementation Plan.

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard(s) become effective:

- BES Cyber Asset (BCA)
- BES Cyber System (BCS)
- BES Cyber System Information (BCSI)
- CIP Senior Manager
- Cyber Assets
- Cyber Security Incident
- Cyber System
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate System
- Management Interface
- Physical Access Control Systems (PACS)
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Removable Media
- Reportable Cyber Security Incident
- Shared Cyber Infrastructure (SCI)

- Transient Cyber Asset (TCA)
- Virtual Cyber Asset (VCA)

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions. The intent of the Compliance Dates for Early Adoption of Revised CIP Standards and Definitions section is to permit Responsible Entities the option to comply with the Revised CIP Standards and Definitions prior to the Effective Date. While the Revised CIP Standards and Definitions are designed to be backwards compatible with perimeter-based security, some Responsible Entities may elect to comply early to leverage different security options associated with zero trust architecture.

Effective Date and Phased-in Compliance Dates

The Effective Dates for the Revised CIP Standards and Definitions are provided below. As noted in the General Considerations section above, the standard drafting team determined to clarify initial performance of periodic requirements and permit Responsible Entities to comply with the Revised CIP Standards and Definitions prior to the effective date. These provisions also are provided below.

Revised CIP Standards and Definitions

Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the later of: (1) April 1, 2026; or (2) the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-

---

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

four (24) months after the date the Revised CIP Standards and Definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards.

Compliance Dates for Early Adoption of Revised CIP Standards and Definitions

A Responsible Entity may elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. In such a case, the Responsible Entity shall select one of the following Early Adoption Dates and shall notify the applicable Regional Entities of their selected Early Adoption Date within fifteen (15) calendar days after their selected Early Adoption Date:

Early Adoption Date
Option 1: First day of the first calendar quarter that is six (6) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 2: First day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 3: First day of the first calendar quarter that is eighteen (18) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions

Responsible Entities must comply with applicable Requested CIP Retired Standards until their selected Early Adoption Date. All Responsible Entities, regardless of whether or not they selected an Early Adoption Date, must comply with the Revised CIP Standards and Definitions by the Effective Date.

Planned or Unplanned Changes

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-7, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-7, Attachment 1, criteria.

For unplanned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirement not applicable to Medium impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Retirement Date

Requested CIP Retired Standards

The Requested CIP Retired Standards shall be retired immediately prior to the effective date of the Revised CIP Standards and Definitions in the particular jurisdiction in which the Revised CIP Standards and Definitions are becoming effective.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

~~Implementation Plan~~
Project 2016-02 Modifications to CIP Standards

~~Virtualization | Draft 4~~ Implementation Plan

Applicable Standard(s)

- Reliability Standard CIP-002-7 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-~~Y~~10 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-8 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-8 – Cyber Security – BES Cyber System Logical Isolation
- Reliability Standard CIP-006-7 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-7 – Cyber Security – System Security Management
- Reliability Standard CIP-008-7 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-5 – Cyber Security – Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-4 – Cyber Security – Information Protection
- Reliability Standard CIP-013-3 – Cyber Security – Supply Chain Risk Management
- Proposed new or modified terms listed in the “CIP Definitions ~~Posting Document (~~Project 2016-02~~)”~~ Modifications to CIP Standards Draft 5”.

  These standards and Definitions of Terms used in the versions listed above of the CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

  These standards and new and modified terms used in the standards above will be referenced as the “Revised CIP Standards and Definitions” within the Implementation Plan.

Requested Retirement(s)

- Reliability Standard CIP-002-~~6~~5.1a – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-~~8~~9 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-7 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)

- Reliability Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-6 – Cyber Security – System Security Management
- Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-3 – Cyber Security – Information Protection
- Reliability Standard CIP-013-2 – Cyber Security – Supply Chain Risk Management

These standards and definitions used in the versions listed above will be referenced as the "Requested CIP Retired Standards~~ and Definitions~~" within the Implementation Plan.

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved ~~or retired~~ before the Applicable Standard(s) become effective:

- BES Cyber Asset (BCA)
- BES Cyber System (BCS)
- BES Cyber System Information (BCSI)
- CIP Senior Manager
- Cyber Assets
- Cyber Security Incident
- Cyber System
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate System
- Management Interface
- Physical Access Control Systems (PACS)
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Removable Media

- Reportable Cyber Security Incident
- Shared Cyber Infrastructure (SCI)
- Transient Cyber Asset (TCA)
- Virtual Cyber Asset (VCA)

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions. The intent of the Compliance Dates for Early Adoption of Revised CIP Standards and Definitions section is to permit Responsible Entities the option to comply with the Revised CIP Standards and Definitions prior to the Effective Date. While the Revised CIP Standards and Definitions are designed to be backwards compatible with perimeter-based security, some Responsible Entities may elect to comply early to leverage different security options associated with zero trust architecture.

Effective Date and Phased-in Compliance Dates

The Effective Dates for the Revised CIP Standards and Definitions are provided below. As noted in the General Considerations section above, the standard drafting team determined to clarify initial performance of periodic requirements and permit Responsible Entities to comply with the Revised CIP Standards and Definitions prior to the effective date. These provisions also are provided below.

Revised CIP Standards and Definitions

Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the later of: (1) April 1, 2026; or (2) the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

---

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Where approval by an applicable governmental authority is not required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the date the Revised CIP Standards and Definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements
Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards~~ and Definitions.~~.

Compliance Dates for Early Adoption of Revised CIP Standards and Definitions
A Responsible Entity may elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. In such a case, the Responsible Entity shall select one of the following Early Adoption Dates and shall notify the applicable Regional Entities of their selected Early Adoption Date within fifteen (15) calendar days after their selected Early Adoption Date:

Early Adoption Date
Option 1: First day of the first calendar quarter that is six (6) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 2: First day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 3: First day of the first calendar quarter that is eighteen (18) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions

Responsible Entities must comply with applicable Requested CIP Retired Standards ~~and Definitions~~ until their selected Early Adoption Date. All Responsible Entities, regardless of whether or not they selected an Early Adoption Date, must comply with the Revised CIP Standards and Definitions by the Effective Date.

Planned or Unplanned Changes

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-7, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-7, Attachment 1, criteria.

For unplanned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirement not applicable to Medium impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Retirement Date

Requested CIP Retired Standards ~~and Definitions~~

The Requested CIP Retired Standards ~~and Definitions~~ shall be retired immediately prior to the effective date of the Revised CIP Standards and Definitions in the particular jurisdiction in which the Revised CIP Standards and Definitions are becoming effective.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards
Draft 5

The standard drafting team (SDT) is seeking comment on the following new or modified terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

Table 1: Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the Reliable Operation of the Bulk Electric System (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS) **Update is Acronym only.**	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more	

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	reliability tasks for a functional entity.	
BES Cyber System Information (BCSI)	Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	Information about the BES Cyber System(BCS) that could be used to gain unauthorized access or pose a security threat to the BCS. BES Cyber System Information (BCSI) does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BCS, such as, but not limited to, device names, individual IP addresses without context, Electronic Security Perimeter names, or policy statements. Examples of BCSI may include, but are not limited to, security procedures or security information about BCS, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BCS.
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Cyber Security Standards.

Table 1: Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.	Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: • For a high or medium impact BES Cyber System (BCS), compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring Systems; or (4) Shared Cyber Infrastructure; or • Disrupts or attempts to disrupt the operation of a BCS.
Cyber System ***New Definition***		One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	Cyber System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems (BCS), including those not protected by an Electronic Security Perimeter used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS.

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	An electronic policy enforcement point or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System through its Electronic Security Perimeter via a bi-directional routable protocol connection.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated electronic access by a person using a bi-directional routable protocol: • To a Cyber System protected by an Electronic Security Perimeter(s) (ESP); • That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or • To a Management Interface. Interactive Remote Access does not include: • Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or • System-to-system process communication.

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
Intermediate System	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.
Management Interface ***New Definition***		An administrative interface that: • Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; • Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or • Configures an Electronic Access Point.
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers	Cyber Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a	One or more Cyber Assets or Virtual Cyber Assets

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	that: • Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or • Share CPU resources or memory resources with any part of the BCS, excluding Virtual Cyber Assets that are being actively remediated in an environment that isolates routable connectivity from BCS; Excluding Transient Cyber Assets.
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure (SCI), (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, SCI, a network protected by an Electronic Security Perimeter, or a Protected Cyber Asset.
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber	A Cyber Security Incident that compromised or disrupted: • A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity; • An Electronic Security Perimeter of a high or medium impact BCS; • An Electronic Access Control or Monitoring

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	System	Systems of a high or medium impact BCS; or • Shared Cyber Infrastructure supporting a BCS.
Shared Cyber Infrastructure (SCI) ***New Definition***		One or more programmable electronic devices, including the software that shares the devices' resources, that: • Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or • Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization. SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA)	A Cyber Asset or Virtual Cyber Asset (VCA) that is: 1. Capable of transmitting or transferring executable code, 2. Not included in a BES Cyber System (BCS), 3. Not a Protected Cyber Asset (PCA) associated

Table 1: Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
	associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	with high or medium impact BCS, and 4. Connected for 30 consecutive calendar days or less: • On a network protected by an Electronic Security Perimeter (ESP) containing high or medium impact BCS, or • Directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a: ▪ BES Cyber Asset, or ▪ Shared Cyber Infrastructure, or ▪ PCA associated with high or medium impact BCS. Virtual machines hosted on a physical Transient Cyber Asset (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Virtual Cyber Asset (VCA) ***New Definition***		A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure (SCI).

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
		Virtual Cyber Assets (VCAs) do not include: • Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems; • Dormant file-based images that contain operating systems or firmware; and • SCI or Cyber Assets that host VCAs. Application containers are considered software of VCAs or Cyber Assets.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards
Draft 5

The standard drafting team (SDT) is seeking comment on the following new or modified terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

Table 1: Modified or Newly Proposed Definitions

NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the ~~reliable operation~~Reliable Operation of the Bulk Electric System~~.~~ (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS)	One or more BES Cyber Assets logically grouped	

Table 1: Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
Update is Acronym only.	by a responsible entity to perform one or more reliability tasks for a functional entity.	
BES Cyber System Information (BCSI)	Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	Information about the BES Cyber System (BCS) that could be used to gain unauthorized access or pose a security threat to the ~~BES Cyber System~~BCS. BES Cyber System Information (BCSI) does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to ~~BES Cyber Systems~~BCS, such as, but not limited to, device names, individual IP addresses without context, ~~ESP~~Electronic Security Perimeter names, or policy statements. Examples of ~~BES Cyber System Information~~BCSI may include, but are not limited to, security procedures or security information about ~~BES~~BCS, Shared Cyber ~~Systems~~Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the ~~BES Cyber System~~BCS.
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	CIP Standards, CIP-002 through CIP-011.	~~CIP~~Critical Infrastructure Protection Cyber Security Standards~~, CIP-002 through CIP-011.~~.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.	Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: • ~~-~~For a high or medium impact BES Cyber System~~,~~ (BCS), compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, ~~or~~ (3) an Electronic Access Control or Monitoring System; or (4) Shared Cyber Infrastructure; or • ~~-~~Disrupts or attempts to disrupt the operation of a ~~BES Cyber System~~BCS.
Cyber System ***New Definition***		One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber	Cyber ~~Assets~~System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber

Table 1: Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
	Systems. This includes Intermediate Systems.	Systems (BCS)~~. This includes Intermediate Systems.~~, including those not protected by an Electronic Security Perimeter used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	~~A~~An electronic policy enforcement point or a Cyber Asset interface on an Electronic ~~Security Perimeter~~Access Control or Monitoring Systems that ~~allows~~controls routable communication ~~between~~to and from one or more BES Cyber Systems or their associated Protected Cyber Assets~~ outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.~~.
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System ~~from a Cyber Asset that is outside of its associated~~through its Electronic Security Perimeter via a bi-directional routable protocol connection.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within	User-initiated electronic access by a person ~~employing a remote access client or other remote access technology~~ using a bi-directional routable protocol~~. Remote access originates from a Cyber Asset that is not an Intermediate~~ :

Table 1: Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
	any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	• To a Cyber System ~~and not located within any of the Responsible Entity's~~ protected by an Electronic Security Perimeter(s) ~~or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1)~~ (ESP); • That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber ~~Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants.~~ System; or • To a Management Interface. Interactive ~~r~~Remote ~~a~~Access does not include ~~system~~: • Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or • System-to-system process communication~~s~~.
Intermediate System	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	~~A Cyber Asset~~One or ~~collection of Cyber Assets performing access control~~more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users. ~~The Intermediate System must not be located inside the Electronic Security Perimeter.~~

Table 1: Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
Management Interface ***New Definition***		An administrative interface that: • Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; • Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or • Configures an Electronic Access Point.
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers	Cyber ~~Assets~~Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	One or more Cyber Assets ~~connected using a routable protocol within~~ or ~~on~~Virtual Cyber Assets that: • Are protected by an Electronic Security Perimeter ~~that is~~(ESP) but are not part of the highest impact BES Cyber System ~~within~~(BCS) protected by the same ~~Electronic Security Perimeter. The impact~~

Table 1: Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
		~~rating~~ESP; or • Share CPU resources or memory resources with any part of ~~Protected Cyber Assets is equal to~~ the ~~highest rated BES~~BCS, excluding Virtual Cyber ~~System~~Assets that are being actively remediated in ~~the same ESP.~~an environment that isolates routable connectivity from BCS; Excluding Transient Cyber Assets.
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets~~,~~ or Shared Cyber Infrastructure (SCI), (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, SCI, a network ~~within~~protected by an ~~ESP~~Electronic Security Perimeter, or a Protected Cyber Asset. ~~Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or	A Cyber Security Incident that compromised or disrupted: • ~~-~~A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity; • ~~-~~An Electronic Security Perimeter of a high

Table 1: Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
	- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	or medium impact ~~BES Cyber System; or~~BCS; • ~~-~~An Electronic Access Control or Monitoring Systems of a high or medium impact ~~BES~~BCS; or • Shared Cyber ~~System~~Infrastructure supporting a BCS.
Shared Cyber Infrastructure (SCI) ***New Definition***		One or more programmable electronic devices, including the software that shares the devices' resources, that: • Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or • Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization. SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.
Transient Cyber Asset (TCA)	A Cyber Asset that is:	A Cyber Asset or Virtual Cyber Asset (VCA) that is:

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: - BES Cyber Asset, - network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or - PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	1. ~~c~~Capable of transmitting or transferring executable code, 2. ~~n~~Not included in a BES Cyber System (BCS), 3. ~~n~~Not a Protected Cyber Asset (PCA) associated with high or medium impact ~~BES Cyber Systems~~BCS, and 4. ~~directly c~~Connected for 30 consecutive calendar days or less: - On a network protected by an Electronic Security Perimeter (ESP) containing high or medium impact BCS, or - Directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) ~~for 30 consecutive calendar days or less to a:~~to a: ~~•~~ BES Cyber Asset, ▪ ~~network within an Electronic Security Perimeter (ESP) containing high~~ or ~~medium impact BES Cyber Systems, or~~ ▪ Shared Cyber Infrastructure, or ▪ PCA associated with high or medium impact ~~BES Cyber Systems~~BCS.

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
		~~Examples of~~ Virtual machines hosted on a physical Transient Cyber Asset~~s~~ (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Virtual Cyber Asset (VCA) ***New Definition***		A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include: • Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems; • Dormant file-based images that contain operating systems or firmware; and • SCI or Cyber Assets that host VCAs. Application containers are considered software of VCAs or Cyber Assets.

Unofficial Comment Form

Project 2016-02 Modifications to CIP Standards | Draft 5

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on draft 5 of the **Modifications to CIP standards** by **8 p.m. Eastern, Thursday, November 16, 2023.**

Additional information is available on the project page. If you have questions, contact Manager of Standards Development, Alison Oswald (404) 275-9410.

Background Information

Project 2016-02 (1) addresses the Federal Energy Regulatory Commission (Commission) directives contained in Order No. 822 and (2) considers the Version 5 Transition Advisory Group (V5TAG) issues identified in the CIP V5 Issues for Standard Drafting Team Consideration (V5TAG Transfer Document).

The V5TAG, which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP Version 5 standards and to support industry's implementation activities. During the V5TAG's activities, it identified certain issues with the CIP Reliability Standards that would be better addressed by a standard drafting team (SDT) for the CIP Reliability Standards. The V5TAG developed the CIP Version 5 Transition Advisory Group Issues for Consideration document to formally recommend that the SDT address these issues and consider modifications to the standard language during the standards development process.

Summary of Changes Overview

The SDT reviewed all comments and made modifications to the Reliability Standards and Definitions accordingly. The most extensive changes were made to CIP-010 regarding change management scope. CIP-005 changes were centered around R2 including further clarifications for IRA and the related definitions. CIP-007's changes were centered on the new Requirement Part 1.3 regarding sharing CPU and memory resources in SCI scenarios. CIP-004's changes were to add scoping of systems that include "with IRA" since IRA is no longer dependent on ERC. The changes to CIP-003 were primarily to back out examples that had been added in the TCA section (Attachment 1) in previous drafts due to the number of comments with questions those examples drove.

The proposed new and revised definitions are not balloted separately but are being balloted via the standards. As such, when voting on the standards, ballot body participants will also be voting on the proposed new and revised definitions used in those standards. The definitions are posted in one document among the other ballot materials. CIP-003, CIP-004, CIP-005, CIP-007, and CIP-010 are being balloted again due to either failing ballot or updates needing to be reballoted through industry. The remaining CIP standards that passed the previous ballot (CIP-002, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013) will be included for final ballot as all modifications in the suite of standards are dependent upon each other and must pass as a group.

Questions

In order to allow the SDT to sort responses received by topic, please submit comments with the respective question.

1. The SDT has modified the IRA definition, CIP-005 R2 and CIP-004 Applicable Systems to address IRA in routable to nonroutable (i.e., IP to serial) conversion scenarios. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

2. The SDT modified other (not related to IRA) definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

3. The SDT revised CIP-005 R1 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

4. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

5. The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

6. The SDT revised CIP-003. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

7. The SDT has revised the Implementation Plan to accommodate for the future enforceable date of CIP-003-9. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes
   ☐ No

   Comments:

8. Please provide any additional comments for the standard drafting team to consider, if desired.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-10

September 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-003-10

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-Y. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-Y is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document stated, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to shorten applicability statements within the body of CIP standards with "BCS" as the defined acronym for "BES Cyber System".

Requirement R2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to align security management control requirements with the virtualization changes.

To ensure SCI supporting low impact BCS is afforded equal security controls as the BCS, the SDT added "SCI that supports a low impact BCS".

Attachment 1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to shorten applicability statements within the body of CIP standards with “BCS” as the defined acronym for “BES Cyber System”.

To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a system(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term system(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Attachment 1 Section 2

Rationale

To ensure virtual infrastructure providing electronic access controls for the low impact BCS is afforded equal physical security controls as the physical Cyber Assets that provide electronic access controls for the low impact BCS, the SDT modified this section to include the Virtual Cyber Asset (VCA) where only Cyber Assets had previously been listed.

Attachment 1 Section 3 Part 3.1

Rationale

Part 3.1(i)

To ensure an asset containing a low impact BCS or an SCI supporting a low impact BCS is afforded equal electronic access controls as the low impact BCS, the SDT added “SCI that supports a low impact BCS and a Cyber System(s) outside the asset containing the low impact BES Cyber System (BCS); or the SCI that supports a low impact BCS””.

To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a Cyber System(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term Cyber System(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Part 3.1(ii) To ensure only necessary inbound and outbound electronic access is permitted for SCI that supports a low impact BCS just as is required for access control to the low impact BCS, the SDT adjusted the language to include communications that are between SCI that supports any part of a low impact BCS and a system(s) outside the asset(s) containing the SCI that supports any part of a low impact BCS.

Part 3.1 (iii) The SDT replaced the undefined ‘intelligent electronic devices’ with the defined term ‘Protection Systems’.

Attachment 1 Section 3 Part 3.2

Rationale

To ensure SCI supporting low impact BCS are afforded equal electronic access controls for Dial-up Connectivity, the SDT added “or SCI that supports a low impact BCS.” To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the ‘per Cyber Asset capability’ was changed to ‘per system capability.’

Attachment 1 Section 5 Part 5.2

Rationale

The final bullet of Attachment 1 Section 5 Part 5.2.1 was preceded with the language “Review of” to make the requirement for other methods parallel to the five options listed above it.

Attachment 1 Section 5 Part 5.3

Rationale

To enable for virtualization technologies and capabilities the SDT added, “or VCA” in Attachment 1 Section 5 Parts 5.3.1.

To ensure SCI supporting a low impact BCS are afforded equal protections from malicious code when using Removable Media, the SDT added “SCI that supports a low impact BCS” to the low impact BCS in Attachment 1 Section 5 Parts 5.3.1 & 5.3.2.

Attachment 2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-Y to shorten applicability statements within the body of CIP standards with “BCS” as the defined acronym for “BES Cyber System”. Additional changes were to align the Attachment 2 Measures with the modifications to the Attachment 1 requirement language.

Technical Rationale from Reliability Standard CIP-003-9

Background

In its final report[1] accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact Bulk Electric System (BES) Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through Member Representatives Committee (MRC) Policy Input.

After considering policy input, the NERC Board adopted a resolution[2] to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Foreword Regarding Section 3 and Section 6

When developing the standards language for this SAR, the SDT considered many variables and inputs to draft clear, concise, and meaningful requirements. The SDT considered the scope and variety of entity sizes, functions, organizations, systems and configurations, entity business processes, remote access, local electronic access, remote access architectures and technologies, and data path and communications protocols. The SDT discussed systems used for electronic access, remote vs local electronic access, vendor access accounts and privileges, and optimal time frames for establishing, identifying, determining, and disabling or terminating vendor electronic access.

The SDT reviewed industry comments and draft language suggestions, existing standards, and discussed and deliberated the options and their potential impacts and interpretative values to industry. The SDT recognized that some entities may use the same process, system and/or technology (for vendor electronic access) that is used by entity personnel, or cases where entities use separate processes, systems, or technologies to manage vendor electronic access. The SDT also discussed systems and Cyber Assets owned by vendors but authorized for use on entity networks, vs systems and Cyber Assets owned by entities but used by vendors for electronic remote access. Because of the variety, the SDT focused on allowing entities to identify their particular risks related to remote vendor electronic access and define processes and plans to define and implement security controls to address those risks.

In reviewing the industry comments, the SDT identified, discussed and considered additional terms for clarification, and came to the following conclusions:

1. Electronic remote access: considered remote access as definition and/or remote access vs electronic remote access - as well as onsite vs off-premises remote access. The use of electronic remote access clarifies the remote access using a method (non-physical) which matches existing electronic remote access in other CIP standards.
2. Interactive Remote Access: avoided the existing NERC Glossary of Terms definition in order to prevent applying high and medium impact requirements upon low impact assets and systems.

---

[1] Supply Chain Risk Assessment Report (nerc.com)

[2] FINAL_Minutes_BOT_Open_Meeting_February_2020.pdf (nerc.com)

3. Active: avoided using this term due to potential unintended consequences. The use of "active" may add further requirements upon entities to define, track and document when "active" occurs vs when it does not.
4. Read-only: avoided using this term due to potential unintended consequences. The use of "read-only" may add further requirements upon entities to define and document systems and processes which are read-only from read-write, and where and when read-only access occurs.
5. Vendor: CIP-013 Supplemental Material[3] addresses the term vendor in context with applicable high and medium BES Cyber Systems. The SDT avoided defining the term vendor specifically within the low impact standards to avoid conflicts for entities with high, medium, and low impact systems.

The language developed gives entities the flexibility to define processes to identify and manage vendor electronic remote access for their specific policies, processes, systems, configurations, organizations, operations, and BES Facilities. The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access.

The SDT agreed to retain Section 3 of CIP-003-9 Requirement R2, Attachment 1 and established Section 6 to specifically address low impact vendor electronic remote access, as well as malicious inbound and outbound data communications which may be sourced from or transmitted to vendors. Based on the SAR, the SDT did not include dial-up from Section 3.2.

The language requires an entity to develop and implement a process or processes for identifying vendor electronic remote access, having a method or methods for disabling vendor electronic remote access, as well as methods to detect known or suspicious vendor inbound and outbound malicious communications.

Entities may choose to define systems, applications and/or configurations used by vendors, accounts and privileges, network data communication paths or physical processes for establishing and disabling vendor electronic remote communications. Section 6 provides the flexibility to meet many types of vendor electronic remote access configurations while managing vendor electronic remote access risks.

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine vendor electronic remote access is initiated; and (3) disable vendor electronic remote access when necessary.

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately 66% have external connectivity which often results in the allowance of vendor electronic remote access. As our grid has grown more complex, the use of external parties to support and maintain low impact BES Cyber Systems, equipment and facilities is expected. However, the prevalence of external connectivity across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this vulnerability, the originating FERC Order[4], and the resulting NERC Board resolution[5], the proposed Attachment 1 Section 6, as it relates to the existing Requirement R2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and vendor electronic remote access.

---

[3] CIP-013 Technical Rationale

[4] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[5] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)

Attachment 1 Section 6 Part 6.1 – Determining vendor electronic remote access

The objective of Attachment 1 Section 6.1 is for entities to determine vendor electronic remote access to their low impact BES Asset(s) and/or BES Cyber Systems. Such visibility increases an entity's ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor's electronic remote access. The obligation in Section 6.1 requires that entities have one or more methods for determining vendor electronic remote access.

Attachment 1 Section 6 Part 6.2 – Disabling vendor electronic remote access

The objective of Attachment 1 Section 6.2 is for entities to have the ability to disable vendor electronic remote access for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity's assets containing low impact BES Cyber Systems. The obligation in Section 6.2 requires that entities have a method to disable vendor electronic remote access, which in turn supports the security objective to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications from vendors, such that the entity may respond to and remediate any resulting adverse impacts.

This sub section is scoped to focus only on vendors' communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with assets containing low impact BES Cyber Systems.

Current obligations in CIP-003-8 Requirement R2 that govern direct electronic communications with low impact BES Cyber Systems are not as robust as those in CIP-005-6 that govern high impact medium impact BES Cyber Systems. Security controls such as use of Intermediate Systems and multi-factor authentication provide additional security protection from malicious communication and overall access controls for high and medium impact BES Cyber Systems. In addition to Intermediate Systems and multi-factor authentication, high and medium impact BES Cyber Systems at Control Centers have requirements to detect malicious communications at the Electronic Access Points of those systems. These security measures are not required at low impact BES Cyber Systems.

In keeping with the NERC stated risk-based model, there may be a scenario where a vendor directly communicates with a low impact BES Cyber System. In the event that this connection may be compromised, the inclusion of security requirements to detect malicious communications under CIP-003-9 Attachment 1 Section 6 would provide entities visibility and opportunity in detecting and mitigating risks posed by vendor communications.

Background Section from Reliability Standard CIP-003-8

The section 6. Background has been retired, removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Guidelines and Technical Basis from Reliability Standard CIP-003-8

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-003-8 to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity’s management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC’s cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization’s internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN “split-tunneling” or “dual-homed” workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity’s Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests

- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media
- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Commented [WM1]: Not sure if this was supposed to be security

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only “necessary” inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for “necessary” inbound and outbound electronic access controls may be documented within the Responsible Entity’s cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

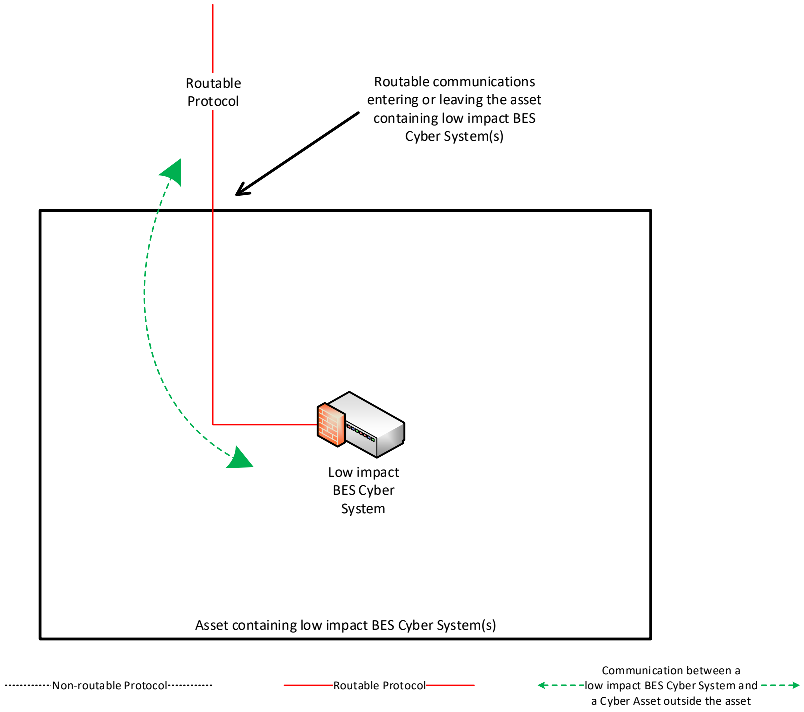
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

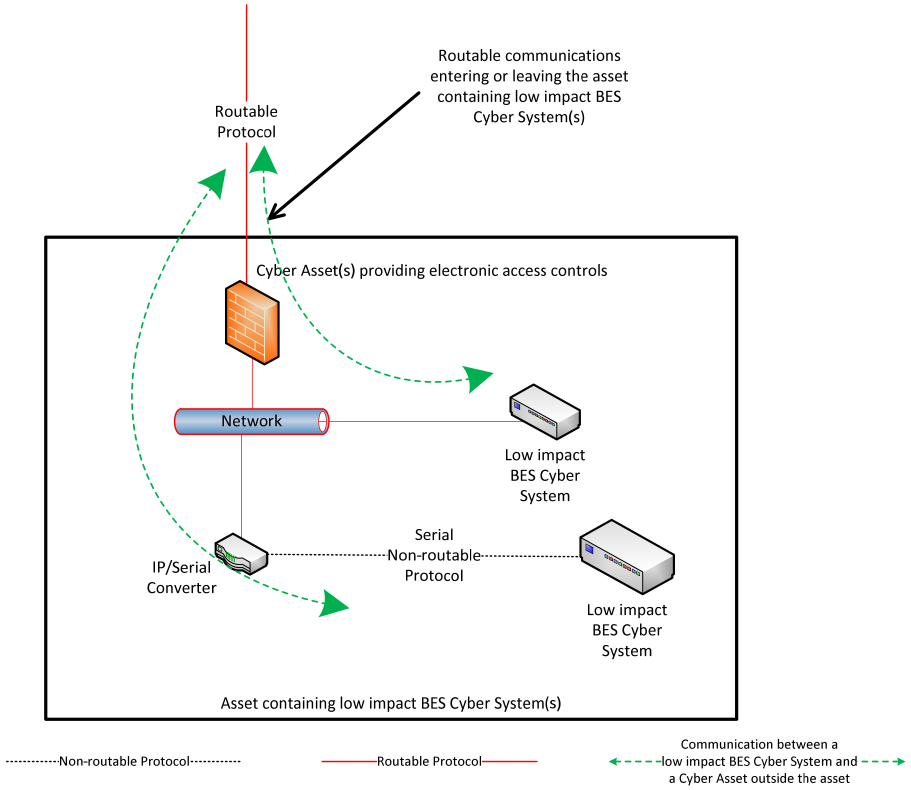
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

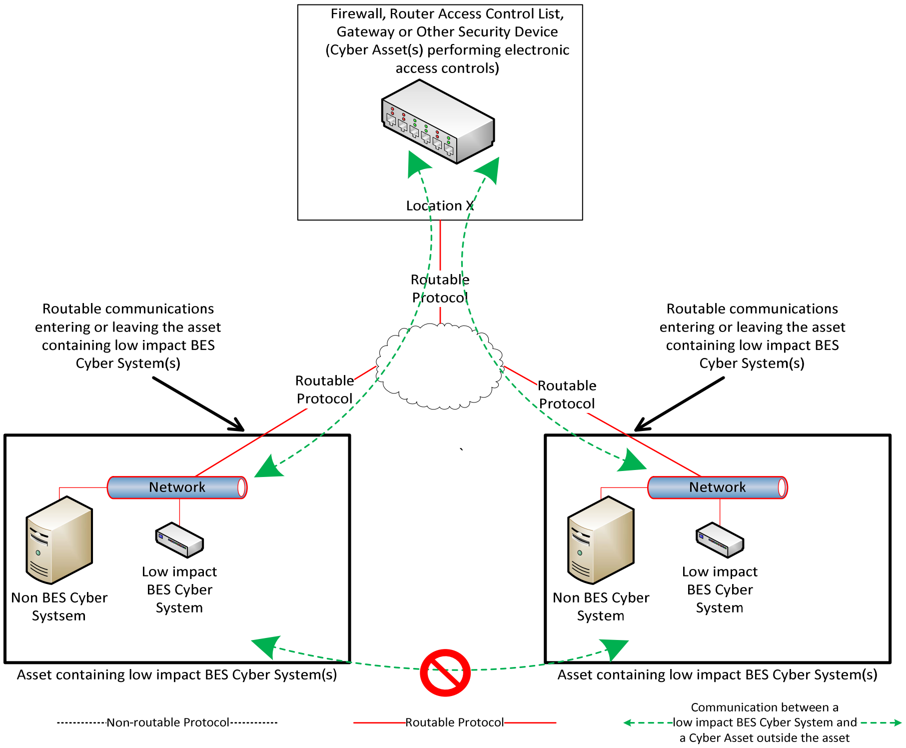
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

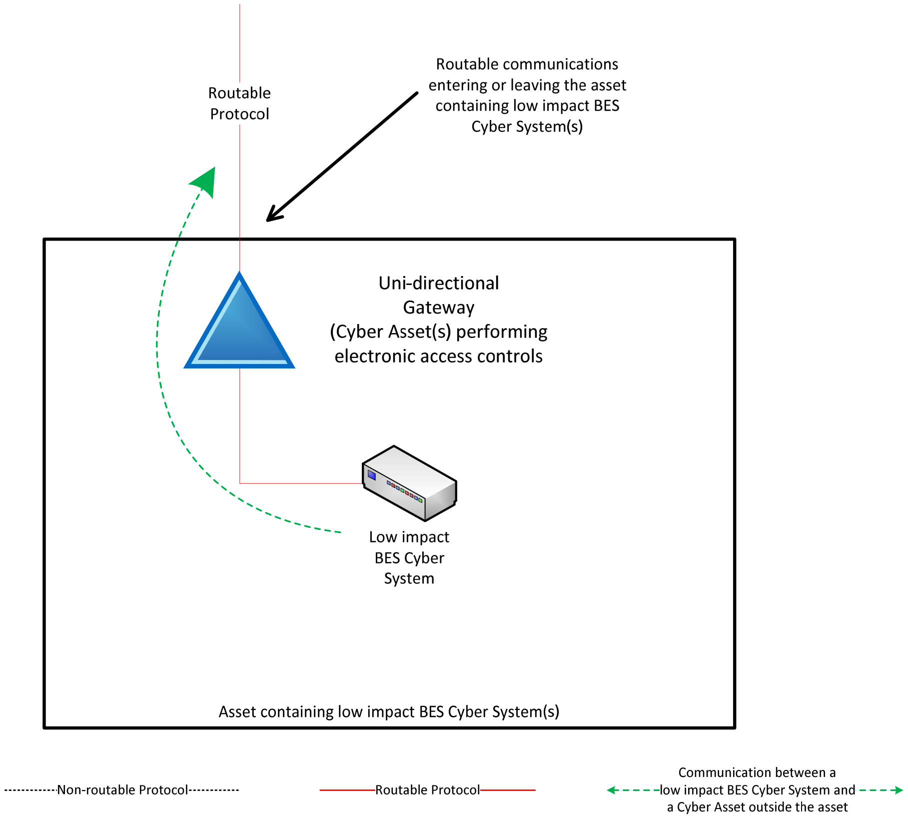
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at “Location X” to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

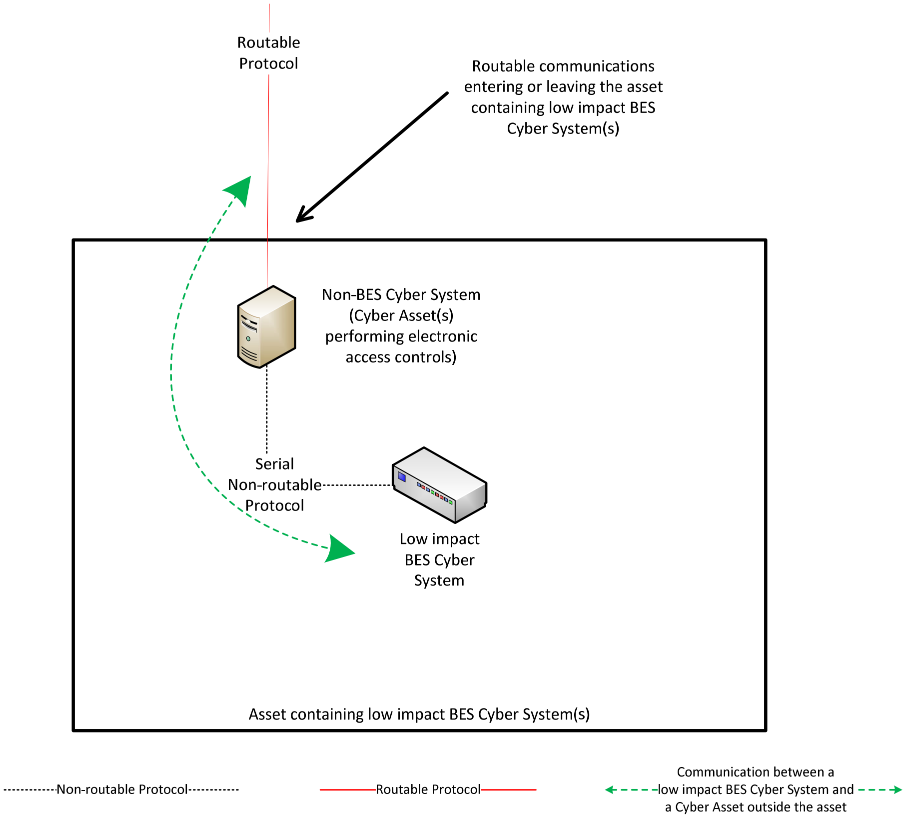
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a “one-way” (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

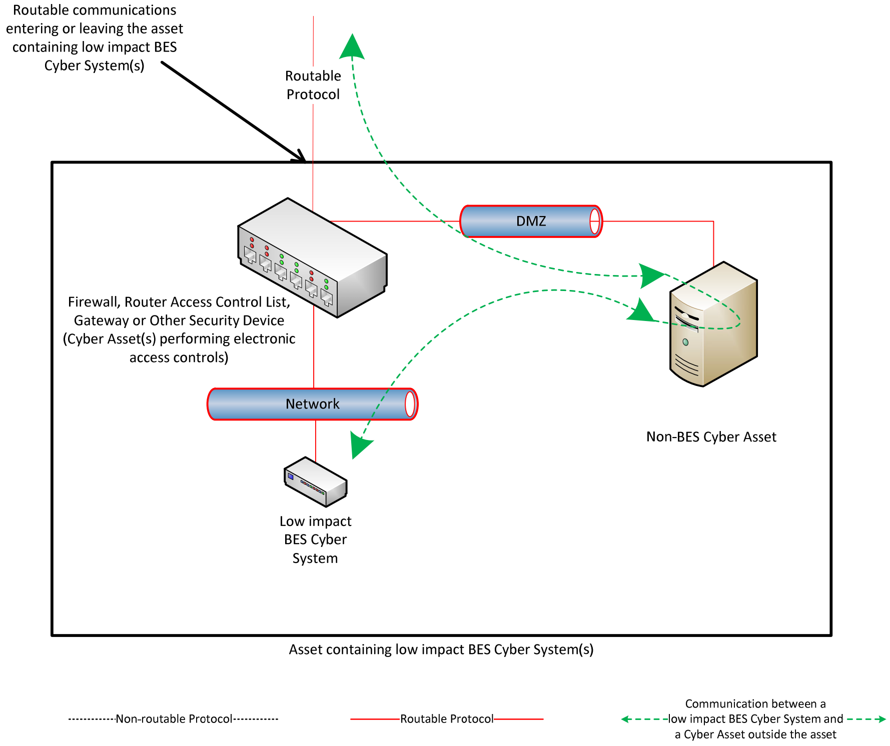
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

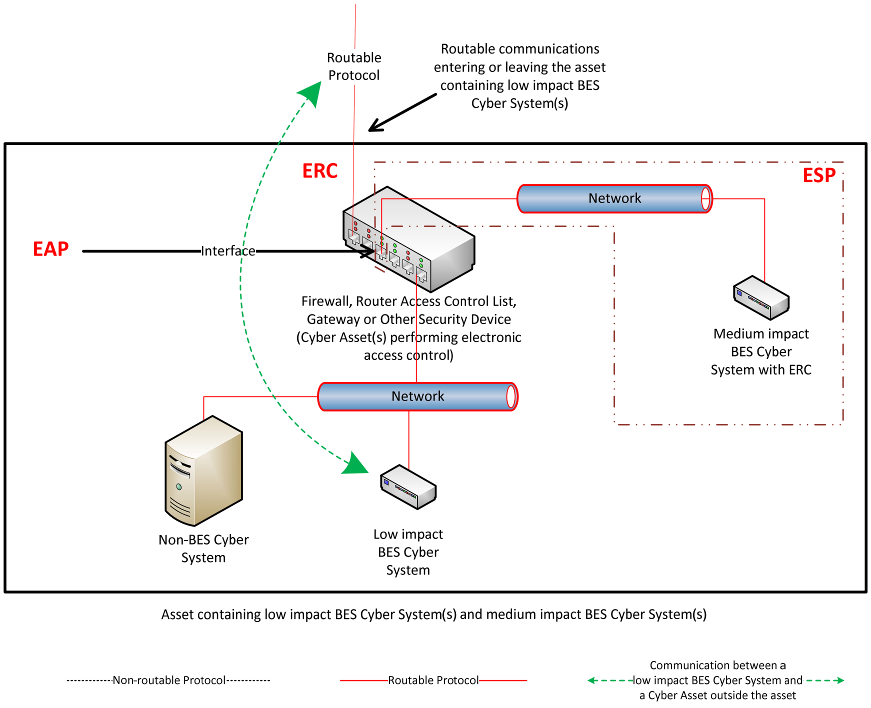
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.



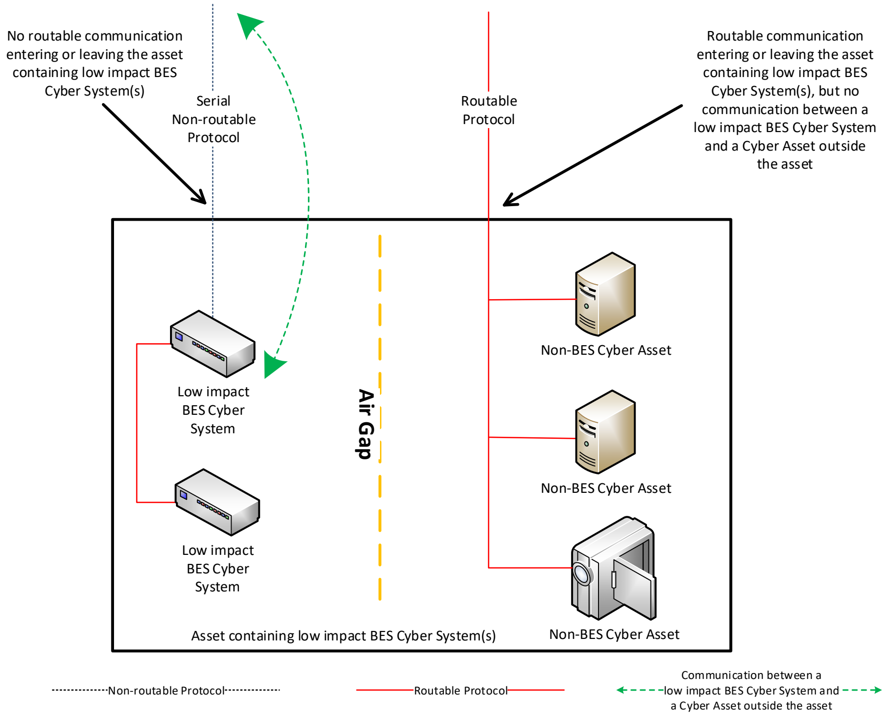
Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).

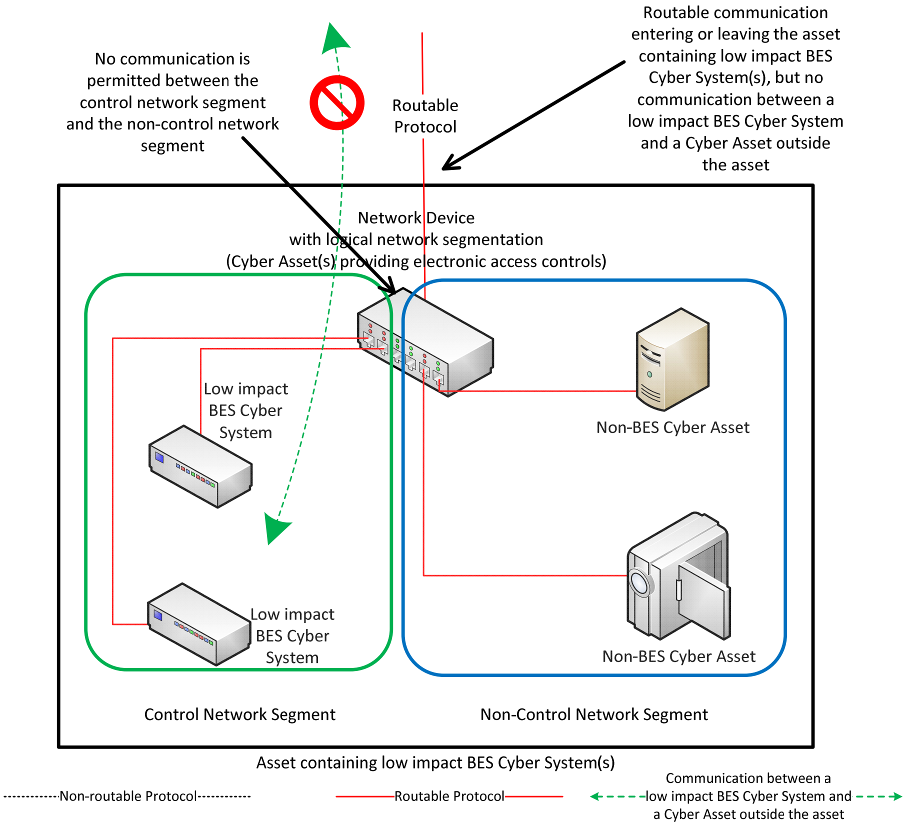
Section 1.



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

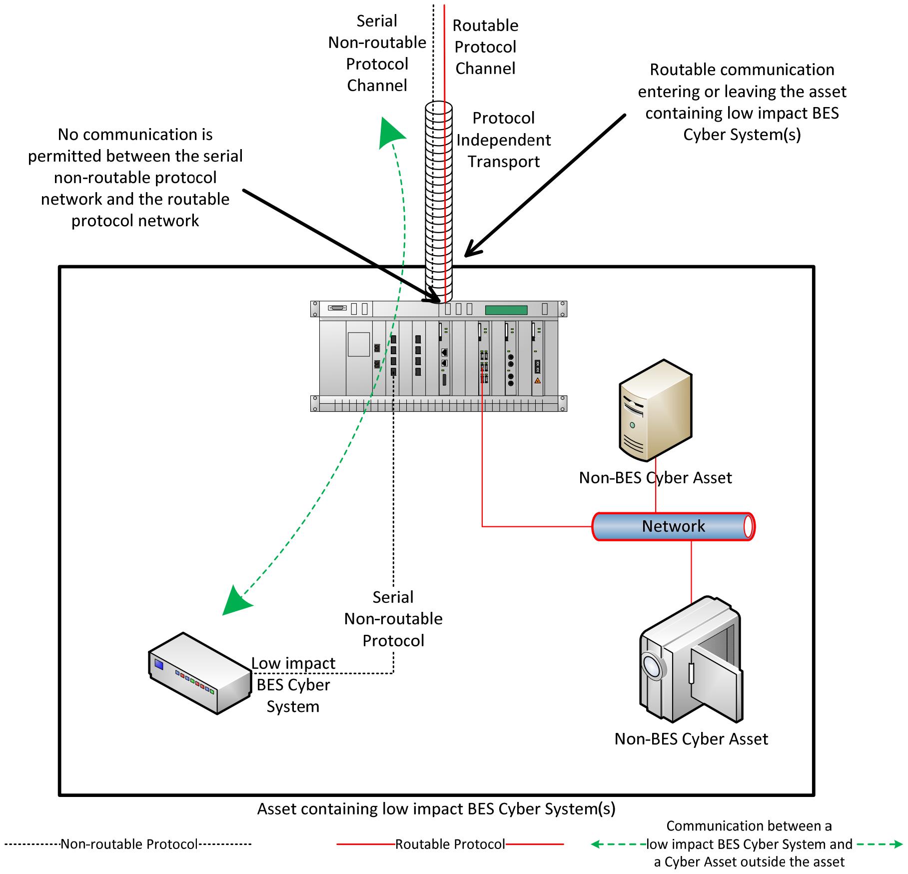
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity’s response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, “A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.” The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[6] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2.1: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Section 5.2.2: The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into

---

[6] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-8

September 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-004-8

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-004-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the issues identified by the V5TAG was virtualization. The V5TAG Transfer document states, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." Document for reference when reading the technical rationale that follows.

Requirement R1-R6

General Considerations

For Requirements R2 through R6, the Project 2016-02 SDT added a new type of 'Applicable System' called '**Medium impact BCS with IRA**'. As the SDT is addressing IRA to a non-routable BCA/BCS through scenarios such as IP-to-serial conversion, IRA is no longer dependent on ERC and "associated ESPs". Therefore, CIP-004 requirements for provisioning and deprovisioning IRA for personnel can no longer be limited to only medium impact BCS with ERC.

However, several of the Requirement Parts cover both physical and electronic access and the "with ERC" has been used as a scoping filter so that, for example, you don't have to deprovision physical access within 24 hours at a remote site that has no ERC and changes for physical security may require a site visit. To account for this situation, several of the Requirement Parts now include a "(except for Medium impact BCS without ERC)" exclusion on the physical access portions of the language.

Note that by adding this to Requirement 2, Part 2.1 it does not mean that all personnel who would ONLY need IRA (i.e., vendors with occasional remote access needs) would need training on all content listed. R2 states the training program is "appropriate to individual roles, functions, or responsibilities".

The Project 2016-02 SDT also made conforming changes to Reliability Standard CIP-004-8 to align personnel and training requirements with the virtualization changes.

To enable CIP-004-8 for virtualization, the SDT added “Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part” within the Applicable Systems column of each of the Parts for Requirement R1 – Requirement R6.

Additionally, where the term BES Cyber System (BCS) was used in the requirement language, it is replaced with “Applicable Systems” to align the requirement language of each Requirement Part with the updated applicability for each Requirement Part.

Requirement R3 Part 3.5

Summary of Changes:

A CIP Exceptional Circumstance was added as an exception to “Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 through 3.4 within the last seven years” such that individuals granted authorized electronic access and authorized unescorted physical access have undergone the personnel risk assessment processes.

Change Rationale:

The SDT determined Responsible Entities cannot require personnel risk assessments for first responders prior to granting them authorized unescorted physical access during certain conditions that qualify as CIP Exceptional Circumstances.

Background Section from Reliability Standard CIP-004-7

The section 6. Background has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:
Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

The following conventions are used in the “Applicable Systems” column as described. High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-004-7

General Considerations for Requirement R1

None

Rationale for Requirement R1

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

General Considerations for Requirement R2

None

Rationale for Requirement R2

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table Requirement R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets (TCA) and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, TCA and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, 7houldd have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least once every 15 months.

General Considerations for Requirement R3

None

Rationale for Requirement R3

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity’s process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new personnel risk assessment (PRA). Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

General Considerations for Requirement R4

None

Rationale for Requirement R4

Authorization for electronic and unescorted physical access must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

General Considerations for Requirement R5

None

Rationale for Requirement R5

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5 Part 5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement R5 Part 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the Bulk Electric System. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

General Considerations for Requirement R6

None

Rationale for Requirement R6

Requirement R6 requires Responsible Entities to implement a BES Cyber System Information (BCSI) access management program to ensure that provisioned access to BCSI is authorized, verified, and promptly revoked. Authorization ensures only individuals who have a need are authorized for provisioned access to BCSI. Prompt revocation of terminated individuals’ ability to access BCSI helps prevent inappropriate disclosure or use of BCSI. Periodic verification ensures that what is currently provisioned is authorized and still required, and allows the Responsible Entity the opportunity to correct any errors in provisioning.

The change to “provisioned access” instead of “designated storage locations” enables the use of third-party solutions (e.g., cloud services) for BCSI. The concept of “designated storage locations” is too prescriptive and limiting for entities that want to implement file-level rights and permissions (i.e., policy based credentials or encryption keys that follow the file and the provisioned individual), which provide BCSI access controls regardless of storage location. The concept of provisioned access provides the needed flexibility for entities to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

According to Requirement R6, Part 6.1, the Responsible Entity must authorize individuals to be given provisioned access to BCSI. First, the Responsible Entity determines who needs the ability to obtain and use BCSI for performing legitimate work functions. Next, a person empowered by the Responsible Entity to do so authorizes—gives permission or approval for—those individuals to be given provisioned access to BCSI. Only then would the Responsible Entity provision access to BCSI as authorized.

Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI.

For BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet. For BCSI in electronic format, electronic access is provisioned to an electronic system or its contents, or to individual files. Provisioned physical access alone to a physical location housing hardware that contains electronic BCSI is not considered to be provisioned access to the electronic BCSI. Take, for instance, storing BCSI with a cloud service provider. In this case, the cloud service provider’s personnel with physical access to the data center is not, by itself, considered provisioned access to the electronic

BCSI stored on servers in that data center, as the personnel would also need to be provisioned electronic access to the servers or system. In scenarios like this, the Responsible Entity should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011-X. The subparts in Requirement R6, Part 6.1 were written to reinforce this concept and clarify access management requirements.

The periodic verification required by Requirement R6 Part 6.2 is to ensure that only authorized individuals have been provisioned access to BCSI and that what is provisioned is what each individual currently needs to perform work functions. For example, by performing the verification, the Responsible Entity might identify individuals who have changed jobs and no longer have a need for provisioned access to BCSI, and would therefore revoke provisioned access.

For Requirement R6 Part 6.3, removal of an individual's ability to use provisioned access to BCSI is considered to mean a process with the result that electronic access to electronic BCSI and physical access to physical BCSI is no longer possible from that point in time onwards using the means the individual had been given to obtain and use BCSI in those circumstances. Either what was specifically provisioned to give an individual access to BCSI (e.g., keys, local user or database accounts and associated privileges, etc.) is taken away, deleted, disabled, revoked, etc. (also known as "deprovisioning"), or some primary access is removed which prevents the individual from using the specifically provisioned means. Requirement R6 Part 6.3 acknowledges that where removing unescorted physical access and Interactive Remote Access, such as is required in Requirement R5 Part 5.1, prevents any further access to BCSI by the individual after termination, then this would constitute removal of an individual's ability to use provisioned access to BCSI. Access can only be revoked or removed where access has been provisioned. The intent is not to have to retrieve individual pieces of BCSI (e.g., documents) that might be in someone's possession (although you should if you can, but the individual cannot un-see what they have already seen).

Where no specific mechanisms are available or feasible for provisioning access to BCSI, these requirements are not applicable. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BCSI, such as when the individual is handed a piece of paper during a meeting or sees a whiteboard in a conference room. Likewise, these requirements are not applicable where provisioned electronic or physical access is not specifically intended to provide an individual the means to obtain and use BCSI. There will likely be no specific provisioning of access to BCSI on workstations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BCSI is only temporarily or incidentally located or stored there. Another example is the provisioning of access to a substation, the intent of which is to enable an individual to gain access to the substation to perform substation-related work tasks, not to access BCSI that may be located there. However, BCSI in these locations and situations still needs to be protected against unauthorized access per the Responsible Entity's information protection program as required by CIP-011-X.

The change to "provisioned access" to BCSI is backwards compatible with the previous "designated storage locations" concept. Entities have likely designated only those storage locations to which access can be provisioned, rather than any location where BCSI might be found. Both concepts intend to exclude those locations where BCSI is temporarily stored, as explained in the previous paragraph. Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of information. The removal of the term "designated storage location" does not preclude an entity from defining storage locations for the entity's access management program for authorization, verification, and revocation of access to BCSI.

Guidelines and Technical Basis from Reliability Standard CIP-004-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.) ;
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least once every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity’s process during the tenure of employment, which may or may not be the same as the initial verification action.

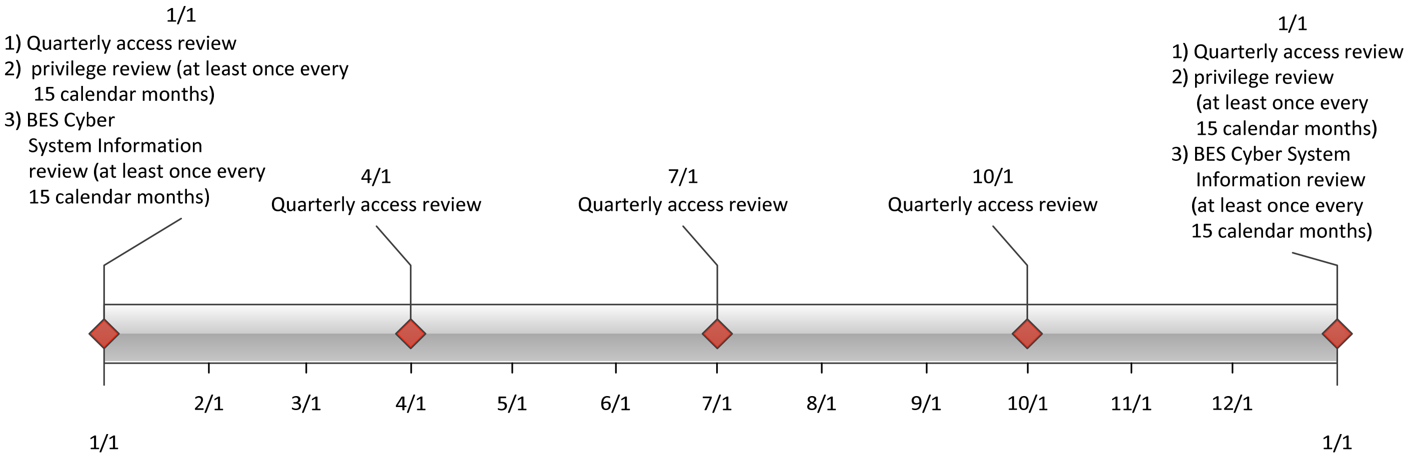
A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.



Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security – Electronic Security Perimeter(s)

Technical Rationale and Justification for Reliability Standard CIP-005-8

September 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-005-8

Introduction

This document is the technical rationale and justification for Reliability Standard CIP-005. It includes the rationale for changes in the current proposed version (CIP-005-8) as well as previous versions of the standard. The intent of this document is to provide stakeholders and the ERO Enterprise with an understanding of the revisions and the technical concepts of the Reliability Standard as well as the rationale for such revisions, both the currently proposed and historical revisions from previous versions and SDTs.

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition Advisory Group (V5TAG), which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005-8 and the definitions of Cyber Asset and Electronic Access Point (EAP) that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

Summary

The Project 2016-02 Standard Drafting Team (SDT) proposal accommodates for increasing use of virtualization and other technology innovation. The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards, but also to better position the CIP standards to be applicable to additional future technological innovation while, to the extent possible, maintaining backwards compatibility.

CIP-005-8 remains a standard concerned with controlling communications to and from BES Cyber Systems (BCS) by establishing an Electronic Security Perimeter (ESP) with increased security controls for Interactive Remote Access (IRA) and vendor remote access. However, virtualization is enabling models for network security, such as "Zero Trust", that are not network perimeter based. Therefore, in CIP-005-8 the ESP focuses on being a security model rather than a network topology-based perimeter as the only option. Securing the communications to and from BCS is the security objective, but the standard no longer prescribes "where", as in where on a network, the controls must be implemented. Innovations such as Zero Trust models are moving access control from network borders to a session level orientation and eliminating the implicit trust within a local network. Network perimeter-based ESP and EAP implementations remain a valid option and are one method for allowing only necessary communications to the Cyber Systems within the ESP.

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in “CIP Definitions and Exemptions Technical Rationale” document for reference when reading the technical rationale that follows.

Requirement R1 General Considerations

ESP Redefined

For backwards compatibility purposes, network border-based ESPs and EAPs remain a valid option for controlling the communications to and from BCS. However, virtualization technologies and models such as Zero Trust present equally effective methods that are not network border-based solutions. A Zero Trust model can implement more granular controls throughout a network on a per-access or per-session level.

Shared infrastructure and “Mixed Trust” Risks

For virtualized environments where SCI is used, a risk of side channel attacks exists. Virtualization allows disparate workloads of what could be differing impact to execute on the same CPUs and share the same memory (i.e., RAM). In this case the lower impact systems would become high water marked with the higher impact system through the PCA definition. This would in turn affect what requires protection by any associated ESPs. The risks associated with this scenario is mitigated in CIP-005-8 by either:

- Declaring the VCAs that share CPU or memory or are within the same ESP with a BCS as associated PCAs which will require they meet the security requirements (high water marking) that include ‘associated PCAs’; or
- Configuring the virtualization infrastructure to place VCAs of differing impact or trust levels into differing CPU and memory pools and configuring affinity controls to these pools such that hypervisors do not allow workloads in these differing pools to simultaneously exist or execute on the same hypervisor.

Assets with Multiple Classifications (PCA, EACMS, Intermediate System, SCI, etc.)

The definitions created to categorize Cyber Assets have historically included overlap. The definition of PCA was revised to include VCAs that share CPU or memory with a BCS. Additional definitions such as SCI and VCA will add to the possibility of additional instances of assets or systems meeting multiple definitions, such as SCI that are also EACMS.

These definitions are used in both the Applicable Systems column as well as within the requirement language. The fact that one asset or system may meet multiple definitions and therefor have multiple classifications does not pose a significant challenge as long as the Responsible Entity ensures that all requirements that pertain to ANY of the classifications are applied. In other words, if an asset or system meets both the SCI and the EACMS definition, requirements that apply to either categorization are applicable.

Firewall/Router on a Stick

A “firewall on a stick” or “router on a stick” is a reference to a networking design scenario by which a firewall or router has one single physical connection to a switch, but has access to multiple networks and broadcast domains by utilizing logical interfaces in combination with VLANs (Virtual Local Area Networks).

Devices on different VLANs are not able to communicate by default, so the primary purpose of this design is to allow for inter-VLAN routing enabling communication between devices which reside on different VLANs by way of the firewall or router.

As all traffic between these VLANs passes through the firewall or router it is uniquely positioned to restrict access and log traffic flows between devices on different VLANs facilitating compliance and the enforcement of security requirements.

This design allows an entity additional flexibility with respect to the creation of multiple Electronic Security Perimeters while minimizing the cost and number of physical networking devices required to provide proper levels of protection and isolation to each of the created Electronic Security Perimeters.

An entity may select this design to enable further isolation of distinct applications and systems from each other based on the assessed risk that they pose to the BES or to enhance their ability to control access to these systems.

Careful attention should be given to the isolation and access control of management interfaces that support this design as they have the potential to impact multiple Electronic Security Perimeters.

SDWAN

Software-Defined Wide Area Networks (SDWANs) are comprised of an underlay network and an overlay network.

The underlay network is what we traditionally refer to as our Wide Area Networks and is constructed with various telecommunications provider circuits and technologies, including Serial, MPLS, LTE, Cable Modem, DSL, etc.

The overlay network is a virtual network layer created upon the underlay network, generally via encrypted tunnels or other similar mechanisms. An overlay network may utilize one or more underlay networks via load balancing or network policies. The policies governing the overlay network may dictate parameters such as what traffic is permitted, what underlay to utilize based on the application type, what should be utilized as the primary path, and various other parameters.

SDWAN enables the construction of secured and isolated network paths with enhanced management and monitoring capabilities in addition to enabling additional services to and from the SDWAN such as VPN connectivity, firewall services, traffic inspection, and shared gateways.

This technology provides an increased level of control over Wide Area Networks while enhancing visibility, security, and redundancy, all while offering the potential to reduce the costs associated with providing connectivity between an entity's locations and assets.

Figure 1 depicts a typical SD-WAN where encrypted tunnels protect traffic between sites A to C as well as sites B to C.

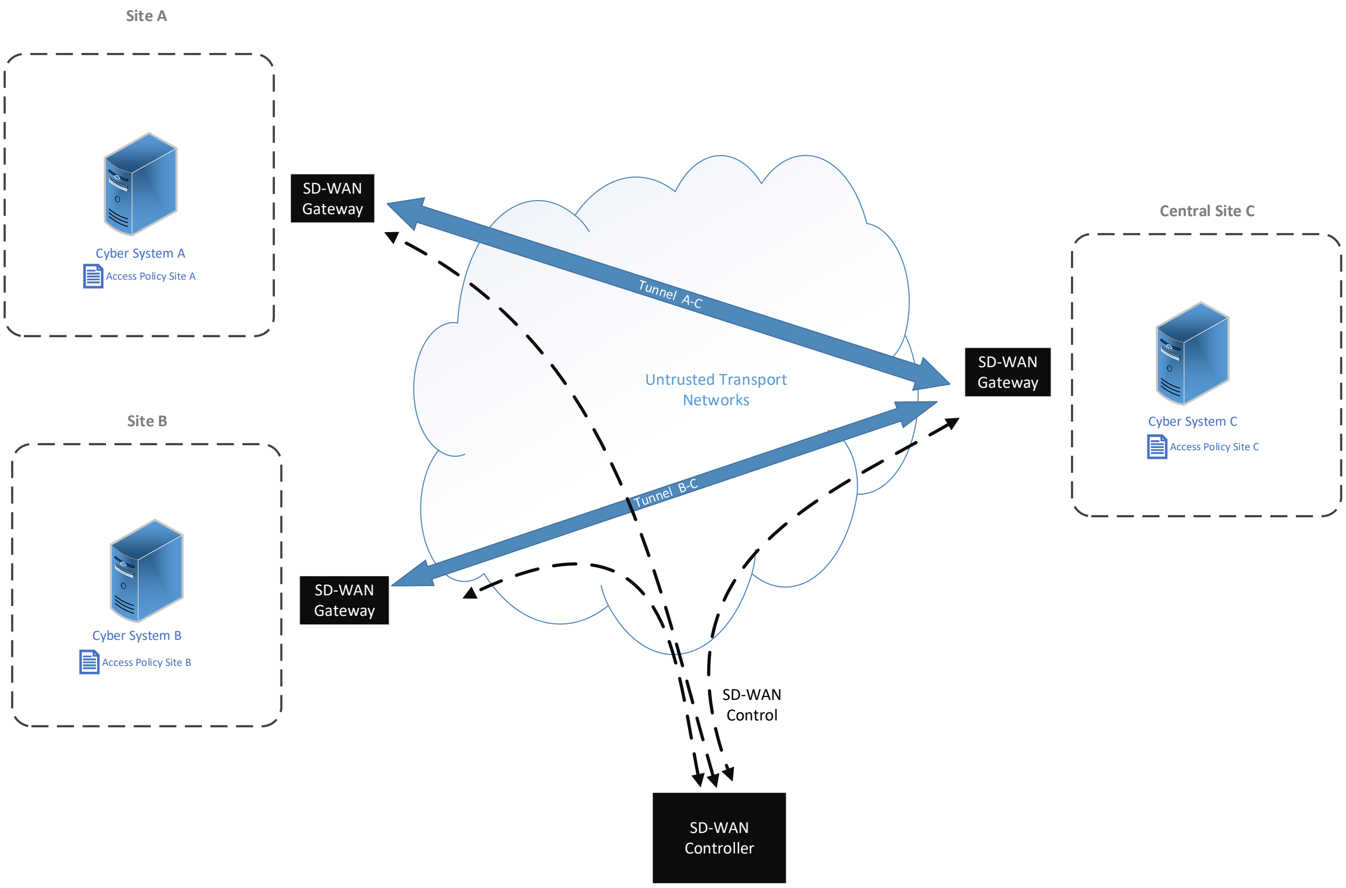


Figure 2 Typical SD-WAN

VXLAN

VXLAN is similar in concept to SDWAN in that it is a form of a Software Defined Network, but in the case of VXLAN the focus is on networks within the Datacenter as opposed to SDWAN which focuses on networks between Datacenters and other facilities.

VXLAN also utilizes the underlay and overlay terminology that we are familiar with given our review of SDWAN. The primary distinction is that VXLAN itself is the name of the overlay protocol utilized in this design and is the most common protocol used for overlay networks within a Datacenter.

The goal of VXLAN is to enhance the ability to segment network resources while also easing the burden of managing, automating, and orchestrating this segmentation by creating a virtual network that is agnostic of the physical network components supporting it.

The VXLAN protocol encapsulates Layer 2 Ethernet frames within Layer 3 UDP packets between devices comprising the design and allows for upwards of 16 million network segments to be created versus the traditional limit of 4094 VLANs. These network segments are identified with a VNI (VXLAN Network Identifier) which is synonymous to a VLAN ID.

The components of the design that are capable of encapsulating and de-encapsulating the VXLAN protocol are referred to as VTEPs (VXLAN Tunnel Endpoints) and are commonly network switches or virtual machine hypervisors.

Physical devices and servers rely on switches to act as their VTEP whereas a virtual machine, hosted on VMWare ESX in this example, relies on the hypervisor as its' VTEP.

Figure 3 depicts a typical VXLAN where access control policies are implemented in the IP fabric.

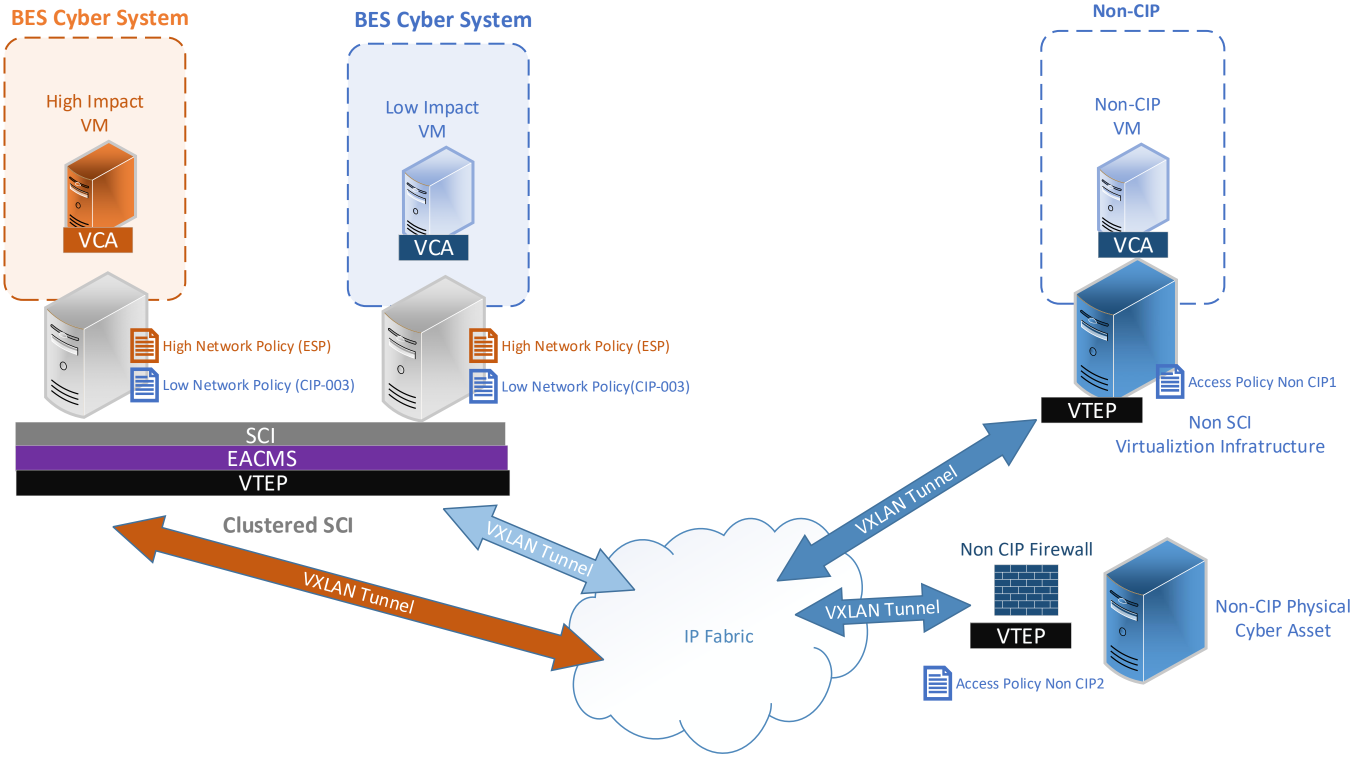


Figure 4 Typical VXLAN

VXLAN facilitates increasing the level of network segmentation within and between an entities Datacenters, while also enhancing their ability to automate and orchestrate the deployment of network resources. With this increased network segmentation an entity is granted more granular control over the flow of traffic and is given more opportunities to inspect that traffic to ensure appropriate levels of access control and protection.

Requirement R1

Rationale

Requirement R1 requires implementation of an ESP for BCS permitting only necessary communication through the ESP. However, there are other network security models available (such as zero trust) that can accomplish this security objective by controlling communications end-to-end at a more granular level than a network perimeter-based model. The definitions (ESP and EAP) and the changes to R1 allow entities the flexibility to implement different models that meet the security objective, or retain their current perimeter-based implementation.

Requirement R1 Part 1.1:

Rationale

This Requirement Part requires all high and medium impact BCS and their associated PCAs be protected by an ESP. In recognition of non-perimeter based models, the language changed from “shall reside within” to “must be protected by”. Note, a PCA can now be defined by two different attributes of what they share with a BCS – not only network location, but also the sharing of CPU and memory from the underlying hypervisor(s) for VCAs. In the instance

that a VCA becomes an ‘associated PCA’ from its sharing of CPU or memory with a high or medium impact BCS, that associated PCA must also be protected by an ESP.

Note that this Requirement Part applies to all high and medium impact BCS without regard to external connectivity from the local network to other networks. This allows for the identification of PCAs and the scope of TCA connectivity even on isolated networks.

Requirement R1 Part 1.2:

Rationale

This Requirement Part changed to a security objective, rather than prescribing ERC must be controlled at an EAP. Virtualization technologies introduce additional methods to isolate systems. This requirement part no longer prescribes one method of controlling communications to Applicable Systems, and opens it up for alternative solutions.

This allows for other models such as zero trust architectures. Such models are not based on controlling communications at a Cyber Asset interface located on a network boundary. Communications can be authorized by software defined policy enforcement points throughout the infrastructure. In this model, network security is less topology-based and more policy-based (configurations and settings) and can be used to granularly protect communication at an individual system or even process or resource level.

While pure zero-trust architectures are an emerging model, the objective-based requirement also allows for hybrid models of various combinations of network border-based and zero trust architectures. As technology changes, this requirement and broadened ESP definition are flexible in how the objective is met.

The core security objective, of permitting only needed communications and denying all others by no longer prescribing this must be implemented at a Cyber Asset interface on a network border (an EAP), is retained. The intent of this Requirement Part is to control the ‘reachability’ of the Applicable Systems; filtering network communications *before* they reach the Applicable Systems and their OS, not as part of it. This is not to discourage the use of integrated host-based firewalls to further filter network traffic to a host.

Note that the requirement now explicitly includes “the reason for granting access”. Previously, this had been an implied part of the requirement based on the Measures.

The SDT had considered adding “physical isolation” to the Measure, but did not do so as the applicability explicitly includes ERC.

Time-sensitive communications between Protection Systems (i.e., digital relays) that use routable communication protocols is excluded. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by inserting an ESP and its controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles (sub-second response times) to protect BES assets. The SDT intent is a Responsible Entity using this technology is not expected to implement the electronic access controls in a situation where it would prohibit the proper function in the proper timeframe.

Requirement R1 Part 1.3:

Rationale

The objective of this new Requirement Part is to protect ESP configurations and SCI configurations. The intent is preventing unauthorized changes to these important configurations by controlling what can connect to administrative interfaces for SCI and certain EACMS.

This can be done by permitting only needed communications to the Management Interfaces, denying all other communications, of the systems that are providing protection of BCS; namely SCI that is supporting an Applicable System from Part 1.1 (SCI isolates systems of different impact levels from each other) and certain EACMS that are controlling an ESP. This Requirement Part only applies to SCI and EACMS controlling an ESP, and not to the BCS itself).

These are vital controls performing the isolation/segmentation between systems of differing impact levels, and warrant protection of the Management Interface that could be used to compromise them.

Certain EACMS that can control access to an ESP are subject to this requirement. This includes those EACMS such as a firewall that is controlling an ESP, a centralized station administering firewalls controlling ESPs as well as a network switch configured with VLANs to isolate and segment traffic. These certain EACMS will need to have their Management Interfaces protected. The SDT intended to exclude EACMS not associated with control an ESP such as domain controllers that provide only authentication services. The SDT is aware of possible implementations where an authentication server is used to provide real-time control of ESP access on a per user basis. In these situations, the authentication server does fall within scope of an EACMS that controls access to an ESP.

The ‘per system capability’ is included in this Part in recognition that some Management Interfaces, such as “ILO” interfaces, may do inbound but not outbound traffic controls.

Requirement R1 Part 1.4:

Rationale

The SDT included “SCI supporting an Applicable System in this Part” to the scope of the requirement part to ensure that controls regarding Dial-up Connectivity are also applicable to VCAs and SCI; and ‘technical feasibility’ has been replaced with the ‘per system capability’.

Additionally, in order to maintain a decipherable Applicable Systems column, the SDT replaced the scoping phrase “with Dial-Up Connectivity” from the Applicable Systems column, with a reference to “if any” in the Requirement Language.

Requirement R1 Part 1.5:

Rationale

Known or suspected malicious communication detection is specific to routable protocol based traffic that enters or leaves the required ESP. Products available to implement this malicious communication detection are usually based on IP traffic (as defined in RFC 791 and upon which TCP and UDP reside). The SDT intended to exclude other data center communications protocols currently in use such as Fibre Channel, where it would not be possible to meet this requirement.

The requirement applicability was changed to the ESP instead of EAPs; lifting it to an objective level and keeping it from being a prescriptive ‘where’ that forces certain architecture.

The SDT had considered adding SCI to the Applicable Systems, however chose not to do so as this functionally may be provided by SCI, thus resulting in a “hall of mirrors” issue. Note that the Management Interfaces of SCI are protected by Requirement R1.3. Entities may wish to implement malicious communications detection on these Management Interfaces of SCI

Requirement R1 Part 1.6:

Rationale

Requirement R1 Part 1.6 was written to address the issue of "Super ESPs" with high or medium impact BCS at Control Centers that extend a single ESP beyond one PSP. This often applies to virtualized Control Center environments that implement network adjacency to allow workloads to automatically move from one physical location to another to increase BCS resiliency between primary and backup Control Centers.

The security objective is to protect the confidentiality and integrity of the data traversing communication links used to span a single ESP between multiple PSPs. This is especially important when portions of the transport are not within the Registered Entity's control. Many encryption methods (such as IPSec and TLS) can fulfil this objective, however some encryption methods fall short of providing both confidentiality and integrity controls.

This Requirement Part works in conjunction with the new 4.2.3.3 exemption in the CIP standards that exempts the Cyber Systems associated with such communication links since the data is required to be protected per this requirement. Also, the former CIP-006-6, Requirement R1, Part 1.10 has been removed and incorporated into this new 1.6 requirement part; consolidating the protections of an ESP and its components that extend outside of a PSP within one standard.

Communications equipment associated with communications links (e.g., equipment belonging to carriers) is exempted from the CIP standards with the 4.2.3.2 exemption, however that only applies to equipment between discrete ESPs. However, in this extended ESP situation where a single ESP spans multiple sites or PSPs, that exemption does not apply and the potential exists for data to traverse a connection that uses third-party communications equipment that is unprotected inside an ESP; hence the need to enforce confidentiality and integrity controls (such as encryption) on the data that traverses PSPs while within the same ESP to isolate any protected data from access through the communications equipment.

This consolidation also incorporates cabling and non-programmable communication components that are not PSP-protected, intending to protect data moving across the state as well as data traversing cabling that crosses the hall outside of the PSP. Note: the language specifically exempts the data that falls under CIP-012 Requirements in order to avoid the potential for double jeopardy as well as the time-sensitive protection or control functions as described in CIP-005-8 Requirement R1 Part 1.1 above.

The SDT had considered adding SCI to the Applicable Systems, however chose not to do so as this functionality may be provided by SCI, thus resulting in a "hall of mirrors" issue.

Requirement R2:

General Considerations for Requirement R2.

External Routable Connectivity (ERC) and Interactive Remote Access (IRA)

The ERC and IRA definitions have been updated in order to:

1. Incorporate new models such as Zero Trust where a security perimeter is not necessarily a network perimeter and ESP's become very granular based on policies that can be established at "people to resource" levels rather than IP address levels.
2. Recognize those Cyber Systems that are of an increased risk due to their "reachability" via ERC and that have IRA available to them even if they are serial-only, non-routable devices.
3. Continue to limit scope of Requirement Parts to BCS with ERC and not those that have connectivity such as non-routable serial leased circuits.

The V5TAG transfer document in the SDT's scope includes the issue of a BES Cyber Asset (BCA) that only uses non-routable protocols over a serial port. These BCAs are not connected to a network with a routable protocol themselves and therefore can be considered to not be within an ESP and thus not have ERC. However, these BCAs can have interactive user access using those serial connections. The SDT's intent is to clarify that IRA can occur to a device with only a serial, non-routable connection through IP-to-serial conversions and be subject to CIP-005-8 Requirement R2. For example, the intent is to clearly cover situations where a serial-only, non-routable BCA, such as a digital relay in a substation, has its serial communication from a 'console port' converted to IP or other routable protocols thus

allowing IRA from users outside the substation to use a routable protocol to interact with the serial device and to require the CIP-005-8 Requirement R2 protection for that IRA.

Due to the inclusion of serial based connections into the revised definition of IRA, other CIP requirements (i.e., CIP-004) have been revised to conform. Entities should review serial/IP converters that are currently being used for remote access.

The SDT removed the requirement-style language "The Intermediate System must not be located inside the Electronic Security Perimeter" from the Intermediate System definition in favor of a clarified objective in CIP-005-8 Requirement R2 that all IRA must be *through* an Intermediate System. Requirement R2 Part 2.6 was added to objectively address the location of the Intermediate System.

See the "*CIP Definitions and Exemptions Technical Rationale*" document for further explanation of the changes to the R2 related definitions.

Requirement R2 Part 2.1:

Rationale

Applicable Systems was updated to include SCI to ensure the same safeguards for remote access methods exist for SCI supporting an Applicable System within the Part as they do for the high and medium impact BCS and associated PCA hosted on that SCI. Backwards compatibility is retained for entities that do not use SCI. Please note that there may be situations where an Intermediate System is implemented as a VCA on SCI. The SDT intends that applicability for SCI is to ensure that the objectives of Requirement R1.3 are met such that the Management Interfaces of SCI are appropriately protected. VCAs are not considered part of SCI and therefore could be used to access a Management Interface of SCI.

The requirement language was simplified, and definitions for IRA and Intermediate System have been updated. Please note that the definition of IRA was changed to include serial communications that are converted to/from routable protocols by the Responsible Entity. This change maintains backwards compatibility except where serial connectivity and routable protocol conversion is being used for IRA.

Requirement R2 Part 2.2:

Rationale

The "Applicable Systems" scope was changed to "Intermediate Systems used to access Applicable Systems in Part 2.1". This clarifies this requirement is associated with the IRA communications between an Intermediate System and the remote clients, as opposed to between the Intermediate System and the BCS. This is important so that it does not require encryption through the ESP to the BCS which would hinder monitoring and inspection.

The requirement was changed from a specific technical-based requirement for encryption to an objective-based requirement to protect confidentiality and integrity of the IRA session between the Intermediate System and the remote client (with encryption as a primary example). The proposed language accounts for the possibility that other equally effective methods could be developed and deployed. This objective also keeps methods from being used that are merely obfuscation methods (XOR, ROT13, etc.) or deprecated encryption methods (DES with 56-bit keys) that no longer meet the objective to protect the confidentiality and integrity of the IRA session.

The changed requirement is backwards compatible except where deprecated encryption methods are in use.

Requirement R2 Part 2.3:

Rationale

The Applicable Systems was changed to “Intermediate Systems used to access Applicable Systems of Part 2.1”. This clarifies this requirement is associated with the Intermediate System itself, and where the requirement for multifactor authentication should be applied (multi-factor authentication to the Intermediate System).

Note that the wording of the requirement was updated to specially apply to IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System. This was previously implied.

Requirement R2 Part 2.4 – 2.5:

Rationale

The applicability and requirements have not changed.

Requirement R2 Part 2.6:

Rationale

This is a new requirement that applies to Intermediate Systems. The intent of this new requirement is to further protect the BCS from the Intermediate System by reducing the attack surface between the two. It is important to note that a virtualized Intermediate System (VCA) hosted in such a way that it can share CPU and share memory with a BCS will also meet the definition of PCA and become an ‘associated PCA’ of the BCS. CIP-005 R1.1 requires that PCA to be within an ESP, in conflict with this requirement. This is by design, and thus a VCA performing the function of an Intermediate System must not share CPU or memory with the BCS it is controlling access for. This is due to the access granted to the less trusted side of the Intermediate System and the risk for side-channel attacks to other VCAs sharing the same CPU and memory. Entities must therefore use affinity rules or some other means to keep Intermediate System VCAs from sharing the same CPU and memory as a BCS or its associated PCAs.

Figure 5 depicts an Intermediate System VCA where an affinity ruleset prevents the sharing of CPU or the sharing of memory with a BES System by ensuring these systems run on different on the hypervisor.

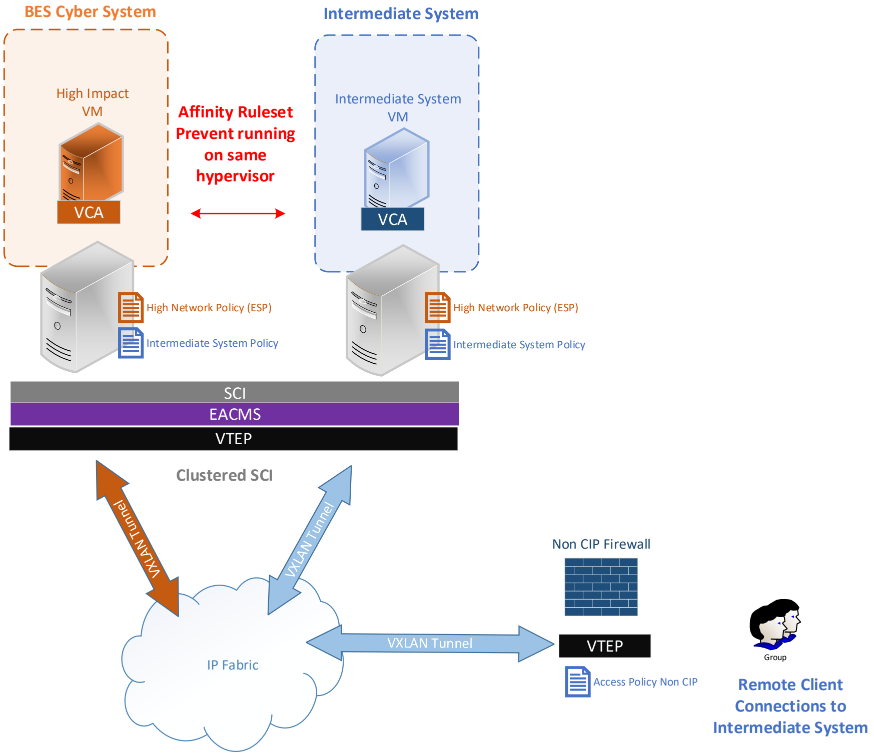


Figure 6 Affinity Rules - Intermediate System does not share CPU or share memory with BES Cyber Systems

Requirement R2 Part 2.7:

Rationale

This is a new requirement that applies to Intermediate Systems. The intent of this new requirement is to further protect the BCS from the Intermediate System by reducing the attack surface between the two. Intermediate Systems have an externally accessible interface that may be used by external parties such as vendors or entity support staff using IRA across an Internet connection to support a remote site. Since Intermediate Systems by nature provide IRA from a less-trusted network and are accessible from yet-to-be authenticated users (in order to authenticate them), a degree of separation from the higher-trust systems they are protecting is necessary in case the Intermediate System is compromised. Previously, this risk was addressed within the glossary definition of Intermediate System ("…must not be located inside the ESP") instead of within an actual requirement. The SDT removed this from the definition and included a security objective in CIP-005-8 Requirement R2 Part 2.7 to require that routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.

Figure 7 depicts an Intermediate System running on non SCI infrastructure. Network connections from the Intermediate System to the BES Cyber Systems must pass through the ESP protecting those systems. In this case, access control policies, implemented on SCI are used to control network connections.

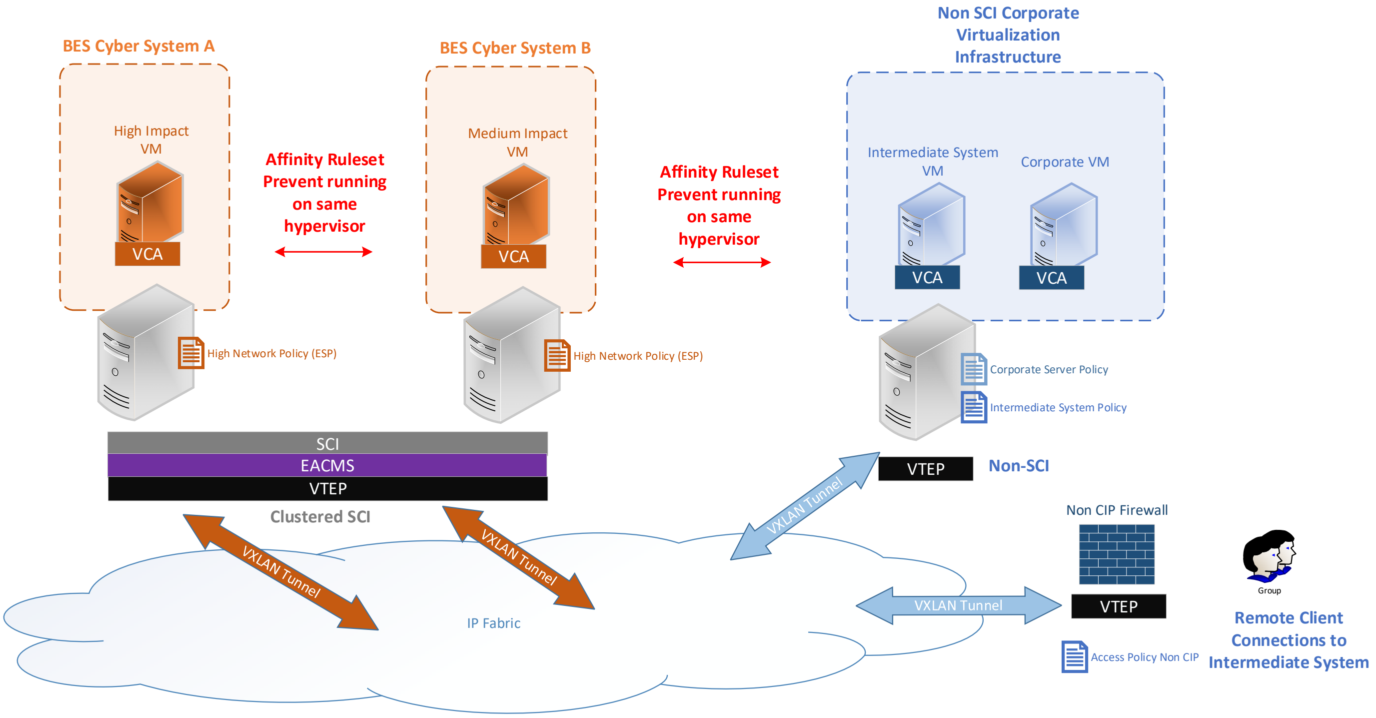


Figure 8 Intermediate System must connect through the Electronic Security Perimeter protecting the BES Cyber Systems

Requirement R3

Rationale

The Applicable Systems section of CIP-005-8 Requirement R3 was updated to include SCI to ensure the same safeguards for vendor-initiated remote connections exist for the applicable SCI. Backwards compatibility is retained for entities that do not currently use SCI.

Background Section from Reliability Standard CIP-005-7

The section 6. Background has been retired. removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BCS and require a minimum level of organizational, operational and procedural controls to mitigate risk to BCS.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BCS. For example, a single training program could meet the requirements for training personnel across multiple BCS.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

Technical Rationale for Reliability Standard CIP-005-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The ESP serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.

But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e., system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the “first line of defense within an Industry Control System (ICS) network environment”. The compromise of those devices that control access management could provide an outsider the “keys to the front door” of the ESP where BES Cyber Systems reside. An intruder holding the “keys to the front door” could use those “keys” to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability

Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[1].

NERC's final report on "*Cyber Security Supply Chain Risks"*, states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

---

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains an as-is "cut and paste" of the former Guidelines and Technical Basis (GTB) from Reliability Standard CIP-005-6 Technical Rationale to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an “Associated Protected Cyber Asset” of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually ‘command and control’ hosts on the Internet, or compromised ‘jump hosts’ within the Responsible Entity’s other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT’s intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity’s address space. The SDT’s intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and ‘deny by default’ type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear ‘perimeter type’ security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions (“TFEs”) rather than increased security.

As for dial-up connectivity, the Standard Drafting Team’s intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.

But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — System Security Management

Technical Rationale and Justification for Reliability Standard CIP-007-7

September 2023

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-007-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-007-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-007-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale.pdf" for reference when reading the technical rationale that follows.

General Considerations

Requirement R1

General Considerations for Requirement R1

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To clarify treatment of virtualization concepts in CIP-007-7, the SDT added "SCI supporting an Applicable System in this Part". This approach keeps the SCI applicability parallel to each existing variant of Applicable Systems in the same Requirement Part (i.e., Medium impact BCS vs. Medium impact BCS with External Routable Connectivity (ERC) vs. Medium impact BCS at Control Centers etc.)

Change Rationale Requirement R1:

The SDT has changed the name of the R1 table to "System Hardening" to more clearly reflect the security objective of the entries in the table, which is to reduce a systems' attack surface. The parts of this requirement do this by:

- limiting network access to only needed routable protocol network accessibility (i.e., logical ports or services),
- limiting access to physical I/O ports (i.e., USB, network, console ports) to only what is necessary, and

- limiting the shared hardware (CPU and memory resources) attack surface between certain groups of VCAs on SCI.

As R1 is broader than only ports and services, the table name was changed to reflect this. The SDT notes that this is merely a label on the Requirement Parts table, linking it to the main Requirement 1 language above it, and does not change or imply any other Requirements or Requirement Parts.

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCA.

Change Rationale Requirement R1 Part 1.1: Requirement R1 Part 1.1 requires "disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability". The SDT updated the Requirement Part language to state a security objective concerning "*routable protocol network accessibility*" as opposed to "ports and services". As this is a new phrase, the intent of this phrase with some examples and rationale for this change is as follows.

> ***Routable protocol network accessibility*** - The objective of this phrase in the Requirement Part is to reduce the attack surface on an applicable system by preventing any unnecessary accessibility to the system over a network using routable protocols. "Accessibility" as used in R1.1 is at the routable protocol network level and does not include physical access, logon to the physical console, code on TCA/RM, etc. Port numbers (TCP/UDP) are at times the best way to track this accessibility, at other times documenting enabled services is better. For example, reducing network accessibility in the physical underlay of SCI between hypervisors or on fabric-based networks may be best performed at a *services* level; turning off or disabling virtualization services that are not needed, rather than documenting the often proprietary and dynamic port numbers which may be of little value. However, in the overlay where an entity may be hosting a database server VCA, it may be easier to show that network accessibility on that VCA is limited to SQL server and remote admin enabled port numbers. In Zero Trust Architectures (ZTA), it may be neither ports or services, but instead a "user to tagged workload" level access control policy where accessibility is described and protected at a more granular, yet higher level than a port #, enforced at a Policy Enforcement Point (PEP) on the applicable system. The SDT has moved to this objective language to avoid prescribing only one way to perform and document network accessibility in all these various scenarios and implementations. In addition, it is limited to routable protocol network accessibility such that non routable network communications (e.g., SAN over Fiber Channel) do not fall within scope of the Requirement Part. The objective is to know the ways a system can be accessed from the network via routable protocols and have no unnecessary attack surface from that perspective.

In this Requirement Part, the SDT used the verbs "Disable or prevent". In some cases, the entity may be able to disable a service or remove/uninstall software that is providing unneeded network accessibility to the applicable system. In other cases, the entity may not be able to disable a service, but can prevent access to it in another layer, such as the underlying OS with a host-based firewall, a PEP, or other means of filtering traffic. In instances where the entity can do neither (e.g., a firmware-based 'black box' device with limited configuration capabilities), the SDT chose to add 'per system capability' to make the requirement conditional on the ability of the applicable system to meet it, if the entity can show that it is incapable.

The SDT also added the clarifier "on each Applicable System" to indicate that the intent of this requirement is for an entity to perform the configuration actions ***on*** each Applicable System, hardening the system from its routable protocol network peers rather than having a single method such as an EAP network firewall rule that would disable such accessibility for a group of Applicable Systems on a network. In other words, merely filtering a port/service on a firewall at an ESP network boundary (CIP-005 R1 controls) does not meet the intent of CIP-007 R1.

Change Rationale Requirement R1 Part 1.3:

Requirement R1 Part 1.3 is a new requirement intended to apply security controls in Shared Cyber Infrastructure scenarios to mitigate the risk of hardware-based vulnerabilities between groups of Applicable Systems of differing impact categorizations. This requirement addresses these vulnerabilities at the CPU and memory level (e.g., Downfall, Inception, Spectre, Meltdown, Rowhammer) that could allow for compromise across processes simultaneously executing on the same shared hardware. Virtualization technology typically has “affinity” controls that can be used to tag VCAs by their impact category and then configure affinity rules such that hypervisors do not instantiate or move VCAs of differing trust levels to the same CPU or memory resources at the same time. Note the requirement excludes shared storage resources, although included in the definition of SCI. The SDT intent is it is allowable to have logical disks attached to systems of differing impact categorization stored in the same SAN for example, and since these storage solutions have internal CPU and memory, that is not the intended object of this requirement.

Note that the SCI definition covers *only* those portions of entity’s virtualization infrastructure that support systems of differing impact levels. As VCAs that share the same CPU or memory with any part of the highest rated BCS are “Associated PCAs” (and thus share the same impact categorization), this requirement is only needed to cover instances where different impact categorizations are supported. This may occur when part of the same SCI supports different BCS and the entity does not wish to high watermark all the BCS together, but instead employ affinity rules to prevent VCAs that are high or medium impact from being instantiated or moved to CPU and memory resources where other VCAs are executing. In this instance the medium impact BCS would still become an associated PCA of the high impact BCS.

For example, this requirement would apply where the same SCI supports both a high impact BCS on one part of a virtualization cluster and a low impact BCS on a different part of the virtualization cluster. The proper use of host affinity controls would not require the low impact BCS to be considered an “associated PCA” of the high as long as:

1. the low impact BCS is not in the ESP of the high impact BCS, and
2. controls are in place to prevent the SCI from executing these BCS on the same CPU and memory resources.

As an example, if an entity has a substation intelligent electronic device (IED) management system that is used as an EACMS for medium and low impact BCS in a single VCA, it is an associated EACMS of the medium impact BCS and protected as such. It can therefore execute on hypervisors with other medium or high impact BCS. If it is implemented as two separate VCAs, one for medium impact IEDs and another for low impact IEDs, then the low impact one cannot execute on the same hypervisor as the medium impact one. Having those two VCAs share the same CPU or memory resources would not meet this requirement. In situations where high or medium impact VCAs are allowed to execute on the same CPU or memory resources with VCA’s of other impact levels and those other VCA’s are inadvertent PCAs, this requirement is a single place for that violation rather than every requirement that has PCA in the scope.

Requirement R2

Change Rationale Requirement R2:

The SDT chose to include the “SCI supporting an Applicable System in this Part” language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA(s) used in applicable BCS, EACMS, PACS or PCA.

The SDT made conforming changes where necessary with Requirement R2 to remove reliance on the Cyber Asset term, choosing to reference the Applicable Systems instead.

Additionally, the SDT chose to insert the word “cyber” as a clarifier to security patches for consistency with the term used in R2.1.

Backward Compatibility

CIP-007-7 Requirement R2 retains backward compatibility for entities that do not utilize SCI.

The SDT intends that entities take full advantage of their virtualization infrastructure in order to ease the overhead associated with patch management. While many of the entity’s existing processes will remain the same, (such as those associated with tracking the source of cyber security patches, evaluation of the applicability of available patches and mitigation plans for those applicable patches that cannot be installed) new or modified processes around the installation of patches can be used (for example, parent images, remediation VLANs, etc.).

Parent Images

One of the interesting nuances of virtualization is the concept of parent/child relationships.

Some VCAs utilize a “parent image” type methodology where a specific VCA (operating system and software) is merely a child instance of a parent image. In such cases, the application of cyber security patches to the parent image applies those changes to any children instantiated from that image. As there may be many dynamic child instances, the administrative overhead associated with patching of those child instances can be greatly reduced. The intent is that entities would track and document the R2 cyber security patching requirements at the parent image level rather than attempting to track and document patching for each individual VCA instantiated from the parent image.

Dormant Instances

There are times when a VCA may not be in use and, as a virtual instance, may be shut down to free its resources since it can be easily instantiated when needed. Thus, VCAs are unlike physical Cyber Assets that are up and running continuously and can receive applicable patches, software updates, configuration updates, etc.

Leveraging the built-in virtualization features allows idle resources to be reassigned to tasks at hand without incurring additional overhead of tracking which dormant virtual instances require patching. Dormant virtual instances are just files with the saved state of the VCA. Dormant instances are not VCAs themselves nor Applicable Systems until they become active instances again.

Where a dormant virtual instance is also the child instance of a parent image, the application of security patches to the parent image will also make the same changes automatically when needed to any out of date dormant child virtual instances when they are restarted.

In most cases, a dormant virtual child instance is made active again on a remediation type network where any missing security patches (compared to the parent image) are automatically applied before it is placed back into active service.

Saved Images

Similar to dormant child images, saved child images or snapshots may be also used as functional backups for CIP-009 purposes in order to provide fast restoration and better availability. If an active VCA becomes corrupted, a saved image can be made active where the application of any missing security patches (compared to the parent image) can be automatically applied, through remediation, before being placed back into active service. However, the SDT’s intent is that VCA images that are used for backup purposes would not be subject to patching, as the backup may be needed to recover from a failed patch or if later discovered that a patch has negatively affected functionality.

Requirement R3

Change Rationale Requirement R3:

The SDT chose to include “SCI supporting an Applicable System in this Part” language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical

Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA.

Requirement R4

Change Rationale Requirement R4:

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA.

Change Rationale Requirement R4 Part 4.1:

The SDT determined the entire structure of the "at the BCS level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)" language could be simplified to "per system capability" since the Applicable Systems column clarifies what systems are included.

Additionally, the SDT chose to insert the word "security" as a clarifier to which events are to be logged.

Change Rationale Requirement R4 Part 4.2:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the "Cyber Asset" term, as well as the ambiguity that would have existed if the term "BES Cyber System" were left in place while the Applicability Column included SCI.

Change Rationale Requirement R4 Part 4.3:

The SDT clarified the retaining of applicable "security" event logs, as that is what is identified in Part 4.1.

The SDT also chose to remove the reliance on a TFE from Part 4.3 in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

Requirement R5

Change Rationale Requirement R5:

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCAs.

Change Rationale Requirement R5 Parts 5.1, and 5.6 – 5.7:

The SDT chose to remove the reliance on TFE in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

Change Rationale Requirement R5 Part 5.4:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the "Cyber Asset" term, replacing it with a per "system" capability.

Change Rationale Requirement R5 Part 5.5:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the "Cyber Asset" term, replacing it with a reference to the Applicable Systems.

Former Background Section from Reliability Standard CIP-007-6

The section 6. Background has been retired, removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rational for Reliability Standard CIP-007-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-007-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

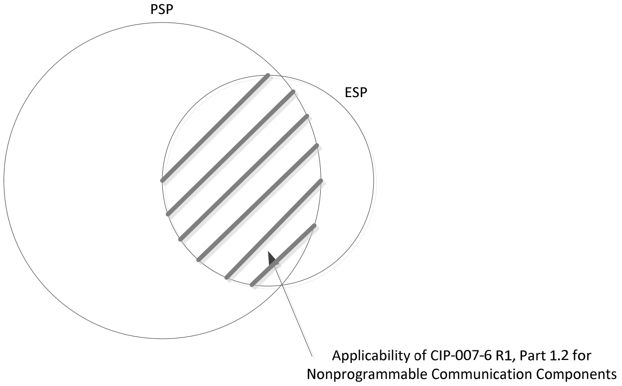
- Disabling all unneeded physical ports within the Cyber Asset’s configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a ‘defense in depth’ type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to “think before you plug anything into one of these systems” which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include “Nonprogrammable communication components located inside both a PSP and an ESP.” This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:

Location of Nonprogrammable Communication Components



Requirement R2:

The SDT’s intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an “install every security patch” requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore, disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Commented [JH1]: Ensure?

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:
Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident.

Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.

- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g., front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g., #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e., as part of the telecommunication carrier's network).

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g., front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit of ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Cyber Security — Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-5

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-010-5

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-5. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-010-5 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference.

Virtualization Concepts Driving CIP-010 Changes

The proposed changes in CIP-010-5 from the Project 2016-02 SDT concern the use of several facets of virtualization technologies. Virtualization allows for such technologies as new controls for Shared Cyber Infrastructure (SCI), remediation VLAN, parent/child images, and dormant virtual machines (VMs). Enabling and clarifying the use of these technologies is the basis of the proposed changes in CIP-010-5. A general introduction to each of these technologies follows.

Shared Cyber Infrastructure (SCI)

Where entries elect to utilize "Shared Cyber Infrastructure", virtualization abstracts the software layers (the OS and applications) from the underlying hardware to allow the hardware infrastructure to be shared among several Virtual Cyber Assets (VCAs) that may be of differing impact levels. Hypervisors must include security controls to keep these workloads logically isolated from one another and those requirements are within other CIP standards such as CIP-005 and CIP-007. However, with any type of shared infrastructure, the need for change management requirements is elevated for those security controls that allow for the 'shared' in SCI. Such controls are added to the change management requirements in CIP-010-5.

As discussed elsewhere, entities may choose to high watermark all VCAs executing in their virtualized infrastructure, known as the "all-in" scenario, and not be concerned with SCI specific requirements. They simply consider the underlay part of the highest impact BCS VCA executing on it and comply with the appropriate security controls and requirements for it.

Remediation VLAN

Remediation VLAN is a term used to describe a logical network segment in which a Cyber Asset or VCA can be isolated from having routable connectivity to any BES Cyber Systems (typically only having visibility of remediation services such as patching and antimalware updates, etc.) while it is examined to ensure the integrity and validity of the configuration and software installed on it. After this examination and subsequent remediation of deficiencies is completed, it is then joined to its production network.

This examination is policy driven, meaning that the administrator is able to configure what the minimum requirements are for a successful examination. Examples of this might be minimum operating system patch levels or recent anti-virus definitions.

If during the examination of the asset, it is found to not comply with the requirements defined in the policy, an administrator may intervene to manually remediate the deficiencies, or the system which was used to examine the asset may communicate the deficiencies to the asset with instructions on how to remediate itself in an automated fashion. After the remediation actions are taken, the asset can request to be re-examined and if the requirements dictated by the policy are now met, it will be joined to its production network.

Parent/Child Images

When a VCA is 'powered on' or begins execution, it instantiates ("boots") from a disk image file. Since the boot 'disk' is a file and not physical disk, many individual VCAs can use the same "parent" image as the basis for their own "child" image. Among other things, this allows for patching of an OS to occur to a parent image and the child images then pick up that patched image upon their next instantiation. A common use of parent/child images is Virtual Desktop Infrastructures (VDI) that deliver a temporary desktop environment to each remote user for the duration of their session that are VCAs instantiated from a parent image.

Dormant VMs

A VCA that is not currently executing or instantiated (i.e., not 'booted up') is a dormant VM. It exists not as a traditional VCA, but simply as a file. VCA's can be created for specialized purposes such as to run troubleshooting tools and are only instantiated when needed and may be dormant for long periods of time. They are not instantiated and on the network where they are managed and patched on a regular basis. However, these can go hand-in-hand with remediation VLANs which would bring them up to date as soon as they do begin to instantiate.

General Considerations

SCI is mutually exclusive from Cyber Assets (CA) by definition. To enable CIP-010-5 for virtualization, the SDT evaluated the existing Applicable Systems and added "SCI that supports an Applicable System in this Part." This approach keeps the SCI applicability parallel to each existing variant of Medium Impact BCS (i.e., Medium Impact BCS vs. Medium Impact BCS with External Routable Connectivity (ERC) vs. Medium Impact BCS at Control Centers etc.).

Requirement R1

General Considerations for Requirement R1

In prior versions, CIP-010 Requirement R1 has required developing a baseline configuration that consisted of five (5) items (OS or firmware, installed and custom software, ports, and patches). The baseline configuration was then used in the remainder of Requirement R1 and R2 as the basis of change management including testing. At a high level, the CIP-010-4 Requirement Part 1.1 was to develop a baseline configuration, Requirement R1 Part 1.2 was to authorize and document changes to the items in the baseline configuration, and Requirement R1 Part 1.3 was to update the baseline configuration within a specific timeframe after a change. This tended to focus the requirement on maintaining documentation of past changes. However, in CIP-010-4 the core security objective of R1 was in Part 1.2 to authorize and document changes and the baseline configuration was used primarily to set the scope of those changes. Maintaining the baseline configuration information within 30 days after making changes is not a security objective, and as we implement more dynamic systems and more automation of change with virtualization, it becomes more problematic.

In CIP-010-5, the SDT considered the more dynamic, policy-based, and automated virtualization technologies discussed in the previous section and determined to focus Requirement R1 on the true security objective of change management and authorizing intended changes. In other words, make R1.2 from version 4 the main focal point in version 5. Maintaining documentation of ever more automated updates to systems after the fact gives way in this version to authorizing changes that will affect the security posture of the system. The SDT is addressing VCA's that may be dormant for long periods of time and dynamically patched at a future instantiation when needed. The SDT considered the focus of R1 is not for entities to track the date/time a VCA may be dynamically instantiated and patched in an automated fashion in a remediation VLAN and then provide evidence that a baseline configuration was updated within 35 days of that dynamic event.

In addition, with the introduction of application containers and orchestration (Kubernetes, Docker Swarms, etc.), application software may no longer be "installed" on a particular OS instance on a particular server. Instead, an orchestration service may instantiate an application container on the best "node" (server with container runtime) at the moment. For example, a dedicated "database server" gives way to a "database service" that can be instantiated in a container on any VCA or CA managed by the orchestrator. Therefore, baseline configurations of statically installed software and open ports loses value as it becomes dynamically managed in these scenarios. The focus of R1 has thus changed from documenting how the VCA is configured at some point post-change to authorizing the changes that will occur to it when it does instantiate, which provides more security value.

Entities may of course continue to maintain and use baseline configurations, but in CIP-010-5 it is no longer the singular prescribed way of setting change management scope and documenting changes. Baseline configurations may continue to be used as evidence for CIP-007 R1 for example, documenting the enabled ports on a system. In fact, baseline configurations will probably continue to be a very common method used by entities to help detect unauthorized changes in CIP-010 R2, but the standard does not prescribe it as the singular way to meet these security objectives. Therefore, the phrase "baseline configuration" has been removed from CIP-010-5 though entities may continue using it as their "how". Again, the focus of R1 in CIP-010-4 and CIP-010-5 is authorizing changes that affect the security posture of the applicable systems; the SDT has just brough it forward as the "what" with baseline configurations as one possible, but not prescribed, "how". Entities may also wish to reference NIST SP 800-128 "Guide for Security-Focused Configuration Management of Information Systems" as a guide for additional information.

The SDT also considered at length the scope of changes that should be subject to R1. In CIP-010-4, the scope was set by the prescribed elements in the baseline config, consisting essentially of software, patches, and ports. As mentioned above, the security objective of putting ports in the baseline configuration is not to document and maintain a list of listening ports; that security objective is covered in CIP-007 R1 to reduce the attack surface by disabling unneeded ports. Maintaining documentation of the patches installed on a system (which becomes more problematic over time with vendor-bundled monthly updates that may install/remove patches differently per each system's needs) is not the security objective. Knowing what patches are available and applicable to the systems and installing them and mitigating the risk is the goal as covered in CIP-007 R2. In CIP-010 R1, authorizing the action in order to manage change is the objective.

In addition, the SDT considered the prescribed list of baseline configuration elements was insufficient as the scope of a change management requirement. For example, in an SCI that is configured to isolate VCAs of different impact levels from each other, managing and authorizing change to that configuration is vital. As Zero Trust architectures come to fruition, managing and authorizing changes to those access policies is crucial. These are all very important security configurations that were not enumerated in CIP-010-4's baseline configuration and thus not in scope. The SDT concluded that creating a longer prescriptive list of items was not appropriate, in that such a list would need to be maintained as technology changes. The SDT decided to put objective language in the requirement and use the Measures to show examples of more detailed lists of items.

Rationale for Requirement R1 Part 1.1

The SDT brought the security objective to the forefront in this requirement part by starting it with "Authorize changes…". Next it narrows the scope to those "that affect Applicable Systems" and the SDT made conforming changes to Applicable Systems to add SCI. The SDT considered that many entities scope their own internal change management processes this way; if a change is to or affects something in their NERC CIP program for medium/highs, it goes through change management. However, the requirement needs a bit more precise scoping so it doesn't include changes such as a user changing their password or desktop background, or a system log being written to hundreds of times an hour. The requirement needs a lower bound, a floor, without attempting to incorporate a prescriptive list of change types or categories.

The SDT used the objective language "…where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 and CIP-007, as defined by the Responsible Entity." The intent is to bound the scope to those changes that affect the system's CIP security posture. More precisely, the intent is to set the floor of the scope to changes that alter the behavior of a cyber security control the entity uses to keep the system secure per CIP-005 and CIP-007 requirements.

The phrasing "alter the behavior of one or more cyber security controls" is intended to help clarify the scope. For example, the intent is that a user changing their password is not in scope; that is a change that may be required on some periodicity by a cyber security control such as a domain password policy but is not a change that alters the behavior *of the control itself*. What would be in scope is a change to that domain password policy.

The "excluding procedural and physical controls" (as well as the "*cyber security* controls" phrase) is intended to exclude from CIP-010 R1's scope changes to controls from CIP-005 and CIP-007 that are not technical controls. An example would be an entity may have signage or port-blockers as a procedural/physical control for meeting CIP-007 R1.2 concerning physical ports. Installing/removing port blockers or changes to the signage is not intended to be subject to CIP-010 R1. A change to the affinity rules for a hypervisor, if the entity uses that in an SCI scenario to meet CIP-007 R1.3, would meet the intent, as well as changes to EAP firewall rules/policy that the entity uses as the control to meet CIP-005 R1. The configuration of anti-malware controls the entity uses, such as update mechanisms or alerting mechanisms that change *how* the control functions in meeting CIP-007 R3 would be included but not the regular signature updates the control uses; those are not changes to the control's configuration that alter the way the control behaves.

Along these lines, rather than including a prescriptive list of change categories or types within the requirement, the SDT did analyze the requirements in CIP-005 and CIP-007 and included examples of cyber security controls that may serve those requirements in the Measures column to help clarify the intent. These are examples and are not a mandatory prescriptive list of the types of changes that would be included and for which evidence of authorization through change records could be provided.

It is important to note the SDT did not include prescriptive timeframes for this requirement. The rationale for this is to account for emergency changes, those that need to occur for reliability of the system when it may not be possible to put in a request and gain authorization beforehand. The SDT intent is for these system reliability related emergency changes to not become a violation of this standard, which it would if it had "prior to" type phrases within it, or required prescriptive definition of what constitutes emergency changes, etc. However, emergency changes will still need to be authorized, after the fact, to meet the requirement.

Rationale for Requirement R1 Part 1.2

Requirement R1 Part 1.2 is where CIP-010-4 Requirement R1 Part 1.5 now lands in CIP-010-5, with minor modifications to Part 1.2.1, and conforming changes to remove the 'baseline configuration' terminology to enable for virtualization.

The SDT chose to remove the reliance on a "Technical Feasibility Exception" in favor of permitting "CIP Exceptional Circumstances" in Pat 1.2.1. The SDT contends testing in a test environment prior to implementing any change in production, and documenting test results may impede Responsible Entities' efforts to recover from events or conditions that qualify as CIP Exceptional Circumstances, and that term still requires an entity to document when that condition occurs with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception (TFE).

Additionally, the SDT chose to add to the phrase "that minimizes differences with the production environment" to eliminate the dependency on baseline configuration.

Rationale for Requirement R1 Part 1.3

Conforming changes to Applicable Systems (see General Considerations above).

Requirement R1 Part 1.3 is where CIP-010-4 Requirement R1 Part 1.6 now lands in CIP-010-5, with conforming changes to remove the 'baseline configuration' terminology and instead referring to operating systems, firmware, software, or software patches changes as the trigger for the Requirement Part.

The SDT acknowledges virtualization vendors may provide a "golden image" to clone multiple other Virtual Cyber Assets as described in the "Parent/Child Images" section above. The SDT intent is for entities that use the golden image technology to account for the software source and integrity of the golden image which covers any unmodified clones derived from it.

Rationale for Requirement R1 Part 1.4

Requirement Part 1.4 is a simplified version of the same part 1.4 in the previous version. The SDT made conforming changes to align the scope of this part with 1.1 with the phrasing "As a part of the changes authorized per Part 1.1…".

It is important to note the SDT intent and rationale behind the wording "As a part of the change". The rationale for that phrase is the entity, before closing out that change, will verify that the change has not adversely affected the cyber security controls. If the entity, as part of the post change verification, finds that it did, the entity must remediate that issue. The intent is this change cannot be completed until it is verified that the cyber security controls are not adversely affected.

What was 1.4.1 in the previous version required the entity to determine, prior to the change, the CIP-005 and CIP-007 controls that might be affected. With the automated remediation technology at instantiation, this is no longer possible and the SDT considered it was not the security objective. The security objective, the required behavior, is that entities ensure that changes don't adversely affect the cyber security controls by verifying them after making the change. That is now the clearly stated focus of 1.4. It is not the SDT's intent that the entity must test *every* cyber security control for *every* change, which is the rationale for the wording "of the altered cyber security controls". If an entity is installing a patch to an application on a BCS, it's not the intent that the entity verify that the domain password policy wasn't changed, however, the entity should verify the patch did not open or enable any unnecessary ports for example. The requirement part 1.4.3 from the previous version to document the results of the verification has been deleted and the SDT rationale is that is essentially a requirement to provide evidence for the actions taken to comply with the requirement part. Therefore 1.4 is now a simplified security objective to be met.

The rationale for the phrasing of "adversely affected" is simply to recognize that the desired effect of a change may be to impact a cyber security control – for example, an entity may wish to change a password policy such that it requires stronger passwords than the CIP standard requires. That would not be an “adverse” change.

Requirement R2

General Considerations for Requirement R2

The SDT has reworked R2 for monitoring for unauthorized changes to work better with the additional scope of R1’s change management. The SDT’s rationale is that all changes that should be included and authorized in a change management program may not have an automated solution for monitoring for unauthorized change and the SDT’s intent is for this requirement’s scope to be items that can be monitored by technical controls. Therefore, the SDT tied R2 loosely to R1’s scope but with a required list of seven cyber security-related categories to monitor. The SDT’s intent is to keep the scope of R2 to those things for which there are automated solutions that can monitor these areas and alert entities to changes.

The SDT has added the term “unauthorized” into Requirement R2 Part 2.1 to focus it on the risk of unauthorized changes. Many implementations will perform this task by monitoring all changes and looking for unauthorized changes within that population. However, the SDT is allowing for a capability that may filter out authorized changes such that the entity can have methods to monitor for unauthorized changes only. The SDT also added “per system capability” in recognition that not all changes in scope can be monitored on every potential in-scope Cyber System. This addition makes the requirement conditional if a system is incapable of monitoring a particular unauthorized change category.

The SDT has used the phrasing “that include at least one cyber security control for each of the following” in order to allow entities to monitor a primary security control if they have multiple overlapping controls. The SDT’s intent is that having multiple security controls over these categories is a good and beneficial practice where possible, and entities should not be discouraged from having more than one. This phrasing’s intent is to allow the entity to choose the primary control they monitor for unauthorized change. The entity may of course do more than one, but one is required.

For the seven required control categories, the SDT notes it intent as follows:

2.1.1 – The intent is to monitor for changes to the system’s configuration affecting ports or services that are enabled such that they provide accessibility via routable protocols on a network interface.

2.1.2 – The SDT notes that the intent of this item is conditional – evidence for this is only required “on SCI.” If there is no SCI, then no control is required. If SCI is in scope, then some control to monitor for unauthorized changes to CPU/memory sharing of VCAs (affinity rules, etc.) is required.

2.1.3 - The intent of this is the traditional monitoring of changes to executable code of the various listed types. As noted in the Measures column, the SDT intends to handle the parent/child image issues by monitoring the parent image from which temporary child images are derived. See the “Parent/Child Images” section earlier in this document for examples.

2.1.4 – The intent is to monitor for unauthorized changes to the configuration of malicious code protection methods, for example whether they have been disabled, or alerting turned off, etc. Note this is not the detection or alerting or remediation of malicious code that is covered in CIP-007; this is monitoring the configuration of your method to ensure its configured behavior has not been changed in an unauthorized manner.

2.1.5 – Similar to 2.1.4, this is not monitoring the security event log and alerting as covered in CIP-007; this is monitoring the configuration of your security event logging and alerting for unauthorized changes that would change its expected behavior (disabling it, changing what is logged, changing where alerts go, etc.)

2.1.6 – The intent of “configuration of authentication methods” is to monitor for configuration changes that affect how a system authenticates its users/processes. Examples would include password policies (not individual user passwords), configuration of multi-factor authentication, changes to Pluggable Authentication Modules (PAM) on Linux systems, etc.

2.1.7 – Along with 2.1.6 concerning how a system is configured to authenticate users, this requires a control to monitor for unauthorized changes to enabled or disabled status of accounts. For example, if a "Guest" account or a default "admin" account have been disabled on a system, monitoring for the unauthorized re-enabling of those accounts.

Requirement R3

Rationale for Requirement R3 Part 3.1

Conforming changes only to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.2

Conforming changes to Applicable Systems (see General Considerations above).

The SDT chose to remove the reliance on a "Technical Feasibility Exception" in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

In Requirement R3 Part 3.2.1, conforming changes have been made to remove the baseline configuration dependency. Additionally, the SDT chose to add to the phrase "that minimizes differences with the production environment" to eliminate the dependency on baseline configuration.

Rationale for Requirement R3 Part 3.3

The previous language of "Prior to adding a new applicable Cyber Asset to a production environment" for the timing of performing a vulnerability assessment has an interesting "chicken or egg" problem when it comes to VCAs. This phrasing for the timing has worked well for hardware "programmable electronic devices" arriving on a loading dock or spares coming in from a warehouse that should be assessed before being physically placed "in production". However, VCA's aren't shipped, they are created in the production environment from a hardware perspective. A VCA image may be created on the hypervisor, an OS installed, the appropriate applications installed, etc., but the VCA is not yet connected to its production network and instantiated in a way that it has connectivity or is performing its function. However, it is from a hardware standpoint in the "production environment" so you can't do an assessment "prior to" that as this is where it's created.

To solve this issue, the SDT replaced this timing phrasing with the language "Prior to becoming a new Applicable System…". The SDT's rationale is the requirement part requires the vulnerability assessment at a point prior to the VCA being instantiated, with the "production" connectivity it requires, to perform its function either as a part of a BES Cyber System or EACMS or PCA. As it begins to perform those functions (i.e., for an EACMS to begin controlling or monitoring electronic access), it becomes an "Applicable System" at that point – prior to that point in time the vulnerability assessment of that VCA should have taken place. The remediation VLAN technologies may perform this automatically at every instantiation. The SDT made this change so that the requirement part did not imply that VCAs had to be created elsewhere, in some other separate hardware environment, assessed, and then somehow imported.

Conforming changes have been made to remove the baseline configuration dependency. The exceptions are "Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System; or CIP Exceptional Circumstances".

Conforming changes made to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.4

Conforming changes made only to Applicable Systems (see General Considerations above).

Requirement R4

General Considerations for Requirement R4

The SDT updated Requirement R4 to include associated SCI into the scope of the required plans for Transient Cyber Assets (TCA) and Removable Media. The SDT also updated Attachment 1, such that the scope is clarified once within Requirement R4 and applies throughout Attachment 1.

The SDT also added an option to the software vulnerability mitigation portions of Attachment 1, Parts 1.3 and 2.1 for “Controls that maintain the state of the operating system and software such that it is in a known state prior to execution”. This option has been added to point to “VM player” type technologies that will run a virtual image as a VCA in an immutable manner, not allowing changes to the image in order to mitigate exploitation of any software vulnerabilities in the image. The SDT’s intent is this is a virtualization-based equivalent to a live operating system booted from read-only media. Virtualization can also offer such options as “snapshots” where any changes to the image are written to a temporary file and discarded when the VCA is shut down, thus restoring it to a pristine state at next instantiation.

The SDT also made several other conforming changes to Attachment 1 for TCAs to ensure continuity in language between the measures and similar sections in CIP-003 Attachment 1.

Former Background Section from Reliability Standard CIP-010-4

The section 6. Background has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicability Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-010-4

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

---

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks*", "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

---

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible.

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-

010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical

Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity’s responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity’s security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity’s plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rationale for Reliability Standard CIP-010-3

This section contains an as-is "cut and paste" of the former Guidelines and Technical Basis (GTB) from Reliability Standard CIP-010-3 to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to “model” the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining

a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible

Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.

- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

UPDATED

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Formal Comment Period Open through November 29, 2023

Now Available

A formal comment period for draft 5 of the **CIP Virtualization standards (outlined below)** is open through **8 p.m. Eastern, Wednesday, November 29, 2023**.

During a review for the upcoming industry webinar, the drafting team found some bullet point placement errors in CIP-003-10 and CIP-010-5 regarding TCAs in Attachment 1. A redline to clean version of draft 4, as well as an updated redline to last posting, redline to last approved, and an updated clean version have been posted on the project page to assist industry in reviewing these corrections.

- CIP-003-10 - Cyber Security – Security Management Controls*
- CIP-004-8 - Cyber Security – Personnel & Training*
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments

*Based on recent board adopted standards for CIP-003-9 and CIP-004-7, the posted versions for the 2016-02 Modifications to CIP Standards reflect CIP-003-10 and CIP-004-8. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-9 and CIP-004-7, the version numbers within this posting are correct and entities will be voting on CIP-003-10 and CIP-004-8.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*

- *Passwords expire every* ***6 months*** *and must be reset.*
- *The SBS* ***is not*** *supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to* ***allow at least 48 hours*** *for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts* ***prior to the last day*** *of a comment/ballot period.*

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **November 20-29, 2023**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager of Standards Development, Alison Oswald (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Formal Comment Period Open through November 16, 2023

Now Available

A formal comment period for draft 5 of the **CIP Virtualization standards (outlined below)** is open through **8 p.m. Eastern, Thursday, November 16, 2023**.

- CIP-003-10 - Cyber Security – Security Management Controls*
- CIP-004-8 - Cyber Security – Personnel & Training*
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments

*Based on recent board adopted standards for CIP-003-9 and CIP-004-7, the posted versions for the 2016-02 Modifications to CIP Standards reflect CIP-003-10 and CIP-004-8. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-9 and CIP-004-7, the version numbers within this posting are correct and entities will be voting on CIP-003-10 and CIP-004-8.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **November 7 - 16, 2023**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager of Standards Development, Alison Oswald (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify "Project 2016-02 Modifications to CIP Standards Observer List" in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Virtualization - Draft 5
Comment Period Start Date:	10/3/2023
Comment Period End Date:	11/29/2023
Associated Ballots:	2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 5 ST

There were 71 sets of responses, including comments from approximately 185 different people from approximately 116 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT modified the IRA definition, CIP-005 R2 and CIP-004 Applicable Systems to address IRA in routable to nonroutable (i.e., IP to serial) conversion scenarios. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

2. The SDT modified other (not related to IRA) definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

3. The SDT revised CIP-005 R1 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

4. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

5. The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

6. The SDT revised CIP-003. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

7. The SDT revised the Implementation Plan to accommodate for the future enforceable date of CIP-003-9. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

8. Please provide any additional comments for the SDT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Jaimin Patal	Saskatchewan Power Corporation (SPC)	1	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Marc Gomez	Southwestern Power Administration (SWPA)	1	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Bryan Sherrow	Board Of	1	MRO

						Public Utilities (BPU)		
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Michael Ayotte	ITC Holdings	1	MRO
Public Utility District No. 1 of Chelan County	Anne Kronshage	6		Public Utility District No. 1 of Chelan County - Voting Group	Anne Kronshage	Public Utility District No. 1 of Chelan County	6	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Rebecca Zahler	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities	4	WECC

						(Tacoma, WA)		
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Nick Fogleman	Prairie Power, Inc.	1,3	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Marcus Perkins	Southern Maryland Electric Cooperative	3	RF
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent	2	NPCC

						System Operator		
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Elizabeth Davis	PJM	2	SERC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Leslie Burke	Southern Company - Southern Company Generation	5	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Jeffrey Streifling	NB Power Corporation	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC

Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
Randy Buswell	Vermont Electric Power Company	1	NPCC
James Grant	NYISO	2	NPCC
John Pearson	ISO New England, Inc.	2	NPCC
Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
David Burke	Orange and Rockland	3	NPCC
Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
Salvatore Spagnolo	New York Power Authority	1	NPCC
Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
David Kwan	Ontario Power Generation	4	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
Glen Smith	Entergy Services	4	NPCC
Sean Cavote	PSEG	4	NPCC
Jason Chandler	Con Edison	5	NPCC
Tracy MacNicoll	Utility Services	5	NPCC

					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	1	NPCC
Shannon Mickens	Shannon Mickens		MRO,SPP RE,WECC	SPP RTO	Shannon Mickens	Southwest Power Pool Inc.	2	MRO
					Mia Wilson	Southwest Power Pool Inc.	2	MRO
					Josh Phillips	Southwest Power Pool Inc.	2	MRO
					Shelly Young	Southwest Power Pool Inc.	2	MRO
					David Minick	Southwest Power Pool Inc.	2	MRO
					Mike Wikerson	Southwest Power Pool Inc.	2	MRO
					Chris Evans	Southwest Power Pool Inc.	2	MRO
					Barry Bull	Southwest Power Pool Inc.	2	MRO
					Rebecca Sanders	Southwest Power Pool Inc.	2	MRO
					Steve Shirley	Southwest Power Pool Inc.	2	MRO

					Cheryl Kirk	Southwest Power Pool Inc.	2	MRO
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power	1	NPCC

						Cooperative, Inc.		
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The SDT modified the IRA definition, CIP-005 R2 and CIP-004 Applicable Systems to address IRA in routable to nonroutable (i.e., IP to serial) conversion scenarios. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.	
Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Edited	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	No
Document Name	
Comment	
CIP-004-7 - R6.1.2 provisioned physical access to physical BCSI (except for BCSI at a medium impact BCS without ERC). The definition which is listed in the CIP-004-8 Technical Rationales and justification states: For BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet. By the NERC definition of “Physical Access” ERC does not exist. The additional language of (except for BCSI at a medium impact BCS without ERC) should be removed since a lockable file cabinet is not able to have External Routable Connectivity (ERC) making this statement mute. The term: Interactive Remote Access (IRA) needs to be defined before it is introduced in a NERC Requirement. It is listed in the Technical Rationale, there is no definition. List the difference between IRA and ERC. If you have ERC, you have IRA. You cannot have either with “Physical Access” as defined as stated above. Remove R6.1.2 and refer to is as access to BCSI whether it is electronic or physical. Make it simple. You either have been granted access to BCSI or you have not. For R4.1.2 it doesn’t matter if the PSP has ERC or not. Access is access. By adding in ERC, it makes the entity to perform more work and create more policies that do not provide any more security. It makes the compliance piece harder to meet while not gaining any security.	

Take guidance from the Nuclear Regulatory Commission (NRC) on Critical Group Membership. You either a critical group member or you are not. Critical group membership allows an individual to work on critical digital assets, whether it is physical or electronical. 1 access control for both types of access.

Medium impact BCS with IRA SCI supporting an Applicable System in this Part – this section needs more clarity on what it is asking the entity to look for. Measures would need to be added to better understand what the ask is.

Likes 0	
Dislikes 0	

Response

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	No
Document Name	

Comment

The SDT has created two different ways of scoping IRA with the current draft of the definition of IRA. In the first case, RE's determine if in-scope IRA exists within the definition, by deciding if the destination Cyber System is inside an ESP (as there are no cases where a Cyber System would be inside an ESP but would not be an Applicable System), while the second case requires RE's to first use the definition to determine if the a protocol conversion is taking place, then use the Applicable Systems of CIP-005 R2 to determine if the destination device is in-scope.

For example, in case 1: An EMS Server (high impact BCA) is inside an ESP. An engineer logs into the EMS server from a jump host outside the ESP. This access meets the first criteria of the definition IRA, and we don't need the Applicable Systems of CIP-005 R2 to determine it is in-scope because all such access would be in-scope.

Case 2: A comm server hosts telnet servers that translate IP to serial for a RTU at a remote site. A employee can initiate a telnet session to the comm server to remotely program the device. This device DOES meet the definition of IRA. But we cannot determine if it is in-scope IRA without knowing the RTU's classification. If the device is low impact or not BES, it is technically IRA, but has no requirements.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. CHPD recommends an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

CHPD's recommendation is as follows:

Definitions:

Interactive Remote Access - User-initiated, interactive electronic access by a person using a bi-directional routable protocol:

- To a routable Cyber System
- That is converted to a non-routable protocol that allows interactive access to a Cyber System
- To a Management Interface

Intermediate System - An Electronic Access Control or Monitoring System(s) that Interactive Remote Access to BES is permitted to originate from.

CIP-005 R2.1

Applicable Systems - High impact BCS and their PCA(s); Medium impact BCS and their PCA(s)

Requirement - Permit Interactive Remote Access (IRA) from outside an ESP, if any, only from an Intermediate System.

CIP-005 R2.2-R2.7 - Unchanged

Thus, all interactive remote access is "IRA", but only IRA that originates from outside an ESP to an Applicable System is in-scope of CIP-005 R2. The system-to-system exemption is no longer needed, as the access has to be "interactive" per the definition of IRA. The ESP-to-ESP exemption is also no longer needed, as that type of communication naturally falls out-of-scope of the updated R2.1 language. And the non-routable concern is brought into the fold by the second bullet point of the definition of IRA.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

FirstEnergy suggests including the following in the proposed IRA Definition:

- User-initiated electronic access by a person using a bi-directional routable protocol:
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System **when conversion is performed by an device located outside of the ESP of the Cyber System**

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No

Document Name	

Comment

SMUD and BANC appreciate the Standard Drafting Team’s work to modify the IRA definition. In the second bullet of the proposed definition, we recommend changing the words “To a Cyber System…” to “To a BES Cyber System…” so that the scope is not expanded to non-BES, EACMS and PACS.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The gap between what is system-to-system communications and what is Interactive Remote Access (IRA) with the new IRA definition should addressed. Entities often rely on IRA ports for system-to-system communication but have not adequately enforced protections or deployed additional internal controls to ensure that malicious actors do not use the ports, or the ports are used later to establish user-initiated remote access. Additional technical measures or controls should be added to a new definition to ensure validity of declared system-to-system communications to Applicable Systems are not used for IRA. In addition, approval of CIP-005-8, with the modified IRA definition, is still conditional, based upon approval of the entire suite of proposed CIP definitions associated with virtualization and SCI terminology. With no formal definition of system-to-system, there is still lingering issues regarding where this fine line between system-to-system and IRA exists. By stipulating system-to-system communications excludes the ability for direct user-initiated electronic access at any time, better delineates IRA from system-to-system communications.

Suggested Interactive Remote Access definition:

User-initiated electronic access by a person using a bi-directional routable protocol:

To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);

That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or

To a Management Interface.

Interactive Remote Access does not include:

Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs; or

System-to-system process communications that cannot be used to establish user-initiated electronic access.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Although IP to Serial Converters are devices within a ESP and PSP environment in which they could be manipulated if the network is compromised, they can not be directly interacted with through interactive remote access. The serial based systems down stream of the converter would only operate on non-routable serial communications protocol. The language as proposed inappropriately brings these non-IRA devices into scope of this requirement.	
Likes 0	
Dislikes 0	
Response	

Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	
Do not agree with the statement, "That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System;" When read, the wording implies that the connection must always be coverted to a non-routable protocol. A more correct statement would be, "To include connections, which are converted by the responsible entity to a non-routable protocol that allows access to a Cyber System".	
Likes 0	
Dislikes 0	
Response	

Ben Hammer - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
The use of a non routable protocol ip to serial does not cover scenarios where an intermediate system is used first to get to the protocol converter. For example, a utility using a centralized EACMS (intermediate server) placed infront of the protocol converter that mitigates the security risks.	
Likes 0	

Dislikes 0	

Response

Sheila Suurmeier - Black Hills Corporation - 5

Answer	No
Document Name	

Comment

Black Hills Corporation requests the standards drafting team consider defining the term “system-to-system process communications” as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying “system-to-system process communications” versus IRA would allow entities to know which controls need to be applied.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

Our recommendation is as follows:

Definitions:

Interactive Remote Access -

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs; or System-to-system process communications that cannot be used to establish user-initiated electronic access.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt

Answer	No
Document Name	

Comment

Black Hills Corporation requests the standards drafting team consider defining the term “system-to-system process communications” as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying “system-to-system process communications” versus IRA would allow entities to know which controls need to be applied.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

Our recommendation is as follows:

Definitions:

Interactive Remote Access -

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs; or

System-to-system process communications that cannot be used to establish user-initiated electronic access.

Likes 0	
Dislikes 0	

Response

Josh Combs - Black Hills Corporation - 3

Answer	No
Document Name	

Comment

Black Hills Corporation requests the standards drafting team consider defining the term “system-to-system process communications” as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying “system-to-system process communications” versus IRA would allow entities to know which controls need to be applied.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

Our recommendation is as follows:

Definitions:

Interactive Remote Access -

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or System-to-system process communications that cannot be used to establish user-initiated electronic access.

Likes 0	
Dislikes 0	

Response

Micah Runner - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

Black Hills Corporation requests the standards drafting team consider defining the term "system-to-system process communications" as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying "system-to-system process communications" versus IRA would allow entities to know which controls need to be applied.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

Our recommendation is as follows:

Definitions:

Interactive Remote Access -

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs; or

System-to-system process communications that cannot be used to establish user-initiated electronic access.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

BC Hydro appreciates the opportunity to review and comment and offers the following.

BC Hydro requests clarity on the definition of Interactive Remote Access (IRA) for the following reason: IRA definition (second bullet) uses the words "To a Cyber System..." which could lead to the understanding that the scope is expanded to non-BES, EACMS and PACS.

BC Hydro proposes that the wording is changed to "To a BES Cyber System..." to make it clear.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

MPC supports comments submitted by ACES.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

NIPSCO does not agree with the proposed definition. The new definition of IRA seems to be virtually the same as ERC. It is a distinction without much of a difference.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO

Answer	No
Document Name	

Comment

Due to the non-routable protocol’s inability to cross an EAP, the definition of Interactive Remote Access (IRA) should not apply. Given this limitation, the ability to cross an EAP to access a Cyber Asset within the ESP should have its definition limited to only routable protocols.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA suggests editing the new IRA definition to say "To a BCS..." in the first bullet point in lieu of just "Cyber Systems" to avoid including other system types such as EACMS, PACS and PCAs.

Likes 0	

Dislikes 0

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1

Answer No

Document Name

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

If the goal is to ensure that user interactive actions, is done remotely(i.e., not in the PSP), on a BCA and PCA, then those actions must go through an intermediate system, and the users must have training, ie CIP-004.

The IRA definition should be simple and not technologically limited (routable vs nonroutable).

The security risks associated to IRA are not dependent on the routable scenarios or routable to nonroutable (i.e., IP to serial) conversion scenarios. They are associated to the remote access.

Furthermore, if the intentionof the IRA definition is to say “Communication that originates from a BCA or a PCA protected by any of the Responsible Entity’s ESPs”, Why is this part of the definition when CIP-005 R1.1 Requires that BCA or a PCA are to be protected by an ESP ?

Also, since CIP-005 R2.4 and R2.5, include System-to-system process communication, I would remove “or System-to-system process communication.” to the definition of IRA as the concept is in the requirements.

SDT should simplify the definition. Suggested improvements include:

IRA: User-initiated electronic access by a person to a BCA or a PCA .

Interactive Remote Access does not include: Out going communication that originates from a BCA or PCA;

The modifications to CIP-004 are adequate.

The modification to CIP-005 R2, more precisely R2.7 is not required, since R1.2 is there to manage all the routable communication. Also R2.7 implies that the converter (IP to Serial) is outside of the ESP. [BCA] – IP – [F/W] – [IPtoSerial] - Serial

Likes 0

Dislikes 0

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer No

Document Name

Comment

Texas RE agrees that IRA definitions and requirements should be modified to address IRA in routable to nonroutable conversion scenarios. Texas RE noticed however, a gap between the glossary definition and the proposed requirements as written, specifically with regards to IRA to SCI.

The SDT has defined IRA as meeting one of the three following criteria:

- User-initiated electronic access by a person using a bi-directional routable protocol to a cyber system protected by an ESP.
- User-initiated electronic access by a person using a bi-directional routable protocol that is converted by the responsible entity to a non-routable protocol that allows access to a cyber system.
- User-initiated electronic access by a person using a bi-directional routable protocol to a management interface.

In CIP-005 R2 Part 2.1 the SDT requires that IRA only be permitted through an Intermediate System. One of the applicable systems is “SCI supporting an Applicable System in this Part.” In CIP-005 R1 Part 1.1 applicable systems are required to be protected by an ESP. SCI is not an applicable system. Since SCI are not an applicable system in CIP-005 R1 Part 1.1 they are not required to be protected by an ESP. An SCI not protected by an ESP will not match the “User-initiated electronic access by a person using a bi-directional routable protocol to a cyber system protected by an ESP” criteria. As such, these communications would not meet the definition of IRA and would therefore be out of scope for CIP-005 R2 Part 2.1.

Texas RE therefore recommends modifying the proposed glossary definition of IRA to include a “User-initiated electronic access by a person using a bi-directional routable protocol to SCI supporting a BCS.”

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AEPC has signed on to ACES comments:

ACES feels the first sub bullet to the IRA definition is overly wordy and is confusing. ACES sugguests:

“To a BCS or a defined Electronic Access Point (EAP).”

The CIP standards are not concerened with IRA to any other systems besides Applicable Systems/BCS, so scoping the definition to just what NERC/CIP’s definition is, does not allow any scope creep.

Likes 0	

Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:
If the goal is to ensure that user interactive actions, is done remotely(i.e., not in the PSP), on a BCA and PCA, then those actions must go through an intermediate system, and the users must have training, ie CIP-004.
The IRA definition should be simple and not technologically limited (routable vs nonroutable).
The security risks associated to IRA are not dependent on the routable scenarios or routable to nonroutable (i.e., IP to serial) conversion scenarios. They are associated to the remote access.
Furthermore, if the intentionof the IRA definition is to say “Communication that originates from a BCA or a PCA protected by any of the Responsible Entity’s ESPs”, Why is this part of the definition when CIP-005 R1.1 Requires that BCA or a PCA are to be protected by an ESP ?
Also, since CIP-005 R2.4 and R2.5, include System-to-system process communication, I would remove “or System-to-system process communication.” to the definition of IRA as the concept is in the requirements.
SDT should simplify the definition. Suggested improvements include:

- IRA: User-initiated electronic access by a person to a BCA or a PCA .
- Interactive Remote Access does not include: Out going communication that originates from a BCA or PCA;

The modifications to CIP-004 are adequate.
The modification to CIP-005 R2, more precisely R2.7 is not required, since R1.2 is there to manage all the routable communication. Also R2.7 implies that the converter (IP to Serial) is outside of the ESP. [BCA] – IP – [F/W] – [IPtoSerial] - Serial

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

By adding the new applicable system of medium impact with IRA in CIP-004 it causes confusion. LCRA believes the intent is to require training and background checks only for individuals with provisioned electronic access to medium impact BCS with IRA; however, it could be construed that any access to these devices requires R2 and R3 to be complied with.

Likes 0	
Dislikes 0	

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	No
Document Name	

Comment

By adding the new applicable system of medium impact with IRA in CIP-004 it causes confusion. LCRA believes the intent is to require training and background checks only for individuals with provisioned electronic access to medium impact BCS with IRA; however, it could be construed that any access to these devices requires R2 and R3 to be complied with.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	No
Document Name	

Comment

There seems to be an inconsistency between EACMS definition and the CIP-005 R2 requirements:

1) {C}EACMS definition includes a protocol converter for BCS where no ESP exists.

2) New R2 Applicable Systems requires an Intermediate System

3) New R2.7 requires an ESP between the Intermediate System and the BCS

Is the intent of the SDT to require the protocol converter to be an Intermediate System? In the case where no ESP exists, then R2.7 cannot be met.

Suggest change the Applicable Systems in R2.1 to exclude situations without ERC or change R2.7 requirements to exclude situations where protocol converter is used and there is no ESP

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments.

There seems to be an inconsistency between EACMS definition and the CIP-005 R2 requirements:
1) EACMS definition includes a protocol converter for BCS where no ESP exists.
2) New R2 Applicable Systems requires an Intermediate System
3) New R2.7 requires an ESP between the Intermediate System and the BCS
Is the intent of the SDT to require the protocol converter to be an Intermediate System? In the case where no ESP exists, then R2.7 cannot be met. Suggest change the Applicable Systems in R2.1 to exclude situations without ERC or change R2.7 requirements to exclude situations where protocol converter is used and there is no ESP

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1,3

Answer	No
Document Name	

Comment

There is a conflict between the newly proposed EACMS which includes "those not protected by an Electronic Security Perimeter used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS" and CIP-005-8 R2.7 that mandates ESP between Intermediate System and High/Medium Impact BCS. Please clarify how to identify ESP when protocol converter is used to connect High/Medium Impact Cyber System serially for IRA from Intermediate System. {C}{C}

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST sees no reason to change the existing approved definition's use of "remote access client or other remote access technology." The second part of the proposed definition would, as written, apply to any remote connection using a communications path that included routable to serial conversion, regardless of where that conversion took place (e.g., remote location vs. "local," or "inside the BES asset" location). If this is what the SDT intends, NST recommends updating the CIP-005 Technical Rationale document to make this clear. NST is also concerned that as proposed, the revised definition could be interpreted to apply to any Cyber System, not just BES Cyber Systems and associated in-scope devices.

Likes 1	Central Hudson Gas &amp; Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC

Answer	No
Document Name	

Comment

There seems to be an inconsistency between EACMS definition and the CIP-005 R2 requirements:
1) EACMS definition includes a protocol converter for BCS where no ESP exists.
2) New R2 Applicable Systems requires an Intermediate System
3) New R2.7 requires an ESP between the Intermediate System and the BCS
Is the intent of the SDT to require the protocol converter to be an Intermediate System? In the case where no ESP exists, then R2.7 cannot be met. Suggest change the Applicable Systems in R2.1 to exclude situations without ERC or change R2.7 requirements to exclude situations where protocol converter is used and there is no ESP

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Tacoma Power is concerned that the exception language in CIP-004 R2 Part 2.3 invalidates the inclusion of the applicable system of “medium impact BCS with IRA”. Tacoma Power recommends deleting the “(except for medium impact BCS without ERC)” from the R2 Part 2.3 requirement language.

Additional editorial comment: “Medium” should not be capitalized in CIP-004 R5 Part 5.1 and R5.2, and R6 Part 6.3.

Likes 0	
Dislikes 0	

Response

Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
It is unclear if a protocol converter meets the proposed definitions for EACMS and EAP. The lack of clarity makes it difficult to apply the new IRA definition when protocol converters are used. The identification of a EAP on a protocol converter could establish an ESP around a BES Cyber System that does not use a routable protocol. The establishment of an ESP would also cause the non-routable BES Cyber System to meet the definition of ERC, which causes a significate increase in the number of applicable CIP requirements.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
This should specifically exclude direct access from a TCA. More detail is needed to understand the scope, for ex: are all serial addresses needed.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
ACES feels the first sub bullet to the IRA definition is overly wordy and is confusing. ACES sugguests: “To a BCS or a defined Electronic Access Point (EAP).” The CIP standards are not concerened with IRA to any other systems besides Applicable Systems/BCS, so scoping the definition to just what NERC/CIP’s definition is, does not allow any scope creep.	
Likes 0	

Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE supports the ISO/RTO Council comments in this area.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The standard drafting team has done a good job in clearly defining the scope of IRA.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the proposed changes for the IRA definition to address IRA in routable to nonroutable (i.e., IP to serial) conversion.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to the IRA definition.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
It appears there may be a discrepancy in the use of BES and BPS. The revised definition of BES Cyber Asset (BCA) includes the following: "Reliable Operatin of the Buld Electric System (BES) while the term Reliable Operation in the Glossary includes: "Operating the element of the Bulk-Power System ..."	
Likes 0	
Dislikes 0	
Response	

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the modifications to the IRA definition, CIP-005 (Requirement R2) and CIP-004 (Applicable Systems) that address IRA in routable to nonrouteable (i.e., IP to serial) conversion scenarios.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes

Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

LaTroy Brumfield - American Transmission Company, LLC - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Rebika Yitna - MEAG Power - 1,3 - SERC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mike Magruder - Avista - Avista Corporation - 1

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. The SDT modified other (not related to IRA) definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

ACES feels the way the definition of Electronic Access Point (EAP) is written in this draft is overly wordy. ACES suggests:

"An electronic policy enforcement point or a Cyber Asset interface on Electronic Access Control or Monitoring Systems that controls routable communication to and from BES Cyber Systems."

ACES feels the way the definition of Intermediate System is written in this draft is overly wordy. ACES suggests:

"Electronic Access Control or Monitoring Systems (EACMS) used to restrict Interactive Remote Access to only authorized users"

ACES also noted that the definition of an Intermidiate System no longer states that it must not be located inside an ESP, combined with the removal of the language from R2.1: "such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset." Without those two statements IRA could be initiated through an ESP to an Intermediate System located in an ESP. ACES feels the removal of the language from the definition and requirement is not what was intended and needs to be added back to ensure the security of IRA. Furthermore

with the removal of the language, it allows a Cyber Asset IRA client to connect directly to Applicable Systems, if the Intermediate System is also an EACMS with an EAP. In this scenario the Cyber Asset client connects to the EACMS using a VPN client and Multi Factor Authentication. Once connected to the Intermediate System, the IRA Client could connect directly to applicable systems. There are other scenarios, but this is the most obvious.

EACMS is already plural. so adding "one or more" to the definition of Intermediate System is redundant.

ACES feels the second bullet point on the new Management Interface should be scoped down. There are a variety of vulnerabilities in "autonomous subsystems" in which one could gain access to a system's console. Changing the scope of the definition to be ONLY those devices specifically designed and or used to allow access to a console would reduce scope creep. ACES suggests:

"Is an autonomous subsystem, specifically designed and or used to provide access to the console independently of the Cyber Asset's CPU, firmware, and operating system;"

ACES feels the first word in bullet point one, section 4, of the TCA definition should be "to" rather than "on"

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

Glossary, changes cause us to read many glossary terms to understand the term, then go to read standard and see how changes to glossary term has impact to the standard.

EX: Management Interface. Definition should include physical interface or process, not both within the same definition.

EX: term ‘unauthorized’ used, focus on the risk of unauthorized change. How is unauthorized defined?

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC

Answer	No
Document Name	

Comment

PCA Definition – routable protocol missing.
Please clarify ESP criteria / demarcation considerations if a Reponsible Entity takes a “policy” or ruleset based approach to an ESP; in relation to PCAs. Examples involving firewall / VLans / Switch controls… Can a Responsible Entity Choose what devices are PCAs based on the policy?
The first bullet is missing the concept of being explicitly connected by a routable protocol
Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or....
Suggest

…. Are connected to a network using a routable protocol and are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST respectfully offers the following comments on proposed new and revised definitions:

Intermediate System: NST recommends maintaining the "not within an ESP" language from the current definition rather than having that component be implied by a requirement part.

Management Interface: NST recommends changing, "An administrative interface,..." to, "A dedicated physical or logical administrative interface,..."

Electronic Security Perimeter: NST believes the proposed new part of the current ESP definition, “or a logical boundary defined by one or more EAPs” is redundant and unnecessary. We therefore recommend maintaining the currently approved ESP definition.

Virtual Cyber Asset: NST suggests including some of the wording found in the definition of "Cyber Asset," such as, "including software and data." NST notes that the proposed definition, as written, would make it possible for a VCA to be hosted on a BES Cyber Asset that is itself a VCA. If this is what the SDT intends, NST recommends modifying the definition to make this clear.

Electronic Access Control and Monitoring System: NST sees no need for modifying the existing definition. We also note that not all protocol converters perform access control and/or monitoring, which makes it inappropriate to include them in a revised definition of EACMS.

External Routable Connectivity: As we did in 2022, NST believes the use of the word, "through (an ESP)" has the potential to cause confusion over the kind(s) of routable communications that may qualify as ERC. ERC to or from a Cyber Asset should be clearly defined as "through" an ESP boundary or access point, not "through" an ESP. The online Merriam Webster dictionary defines "through" as "a function word to indicate movement into at one side or point and out at another and especially the opposite side of // 'drove a nail through the board'". NST believes the existing definition of ERC can and should be retained as-is.

Shared Cyber Infrastructure: NST recommends adding "hardware" to "One or more programmable electronic devices, including the software,..." NST also recommends adding language to either or both of the "Cyber Asset" and "SCI" definitions that clarifies a device that hosts and/or provides storage resources for BES Cyber Systems and associated virtual devices at a single impact level (e.g., high) should be identified as a Cyber Asset, not as SCI.

Electronic Access Point: As we did in 2022, NST believes the proposed definition of EAP is problematic in two respects. First, we believe it could be interpreted to mean an EAP should control all routable communication between a BCS and any other Cyber Asset regardless of whether that "other" device is within or outside of the same ESP protecting the BCS. Second, we believe the SDT should better define "policy enforcement point" lest Responsible Entities, Regional Entities, and NERC develop their own conflicting definitions.

Transient Cyber Asset: As we did in 2022, NST notes the proposed definition includes a statement ("Virtual machines hosted on a physical Transient Cyber Asset (TCA) are treated as software on that physical TCA.") that directly conflicts with a statement included in the proposed definition of Cyber Asset ("VCAs are not considered software or data of Cyber Assets.").

Likes 1	Central Hudson Gas &amp; Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments.

PCA Definition – routable protocol missing.
Please clarify ESP criteria / demarcation considerations if a Reponsible Entity takes a “policy” or ruleset based approach to an ESP; in relation to PCAs.
Examples involving firewall / VLans / Switch controls… Can a Responsible Entity Choose what devices are PCAs based on the policy?
The first bullet is missing the concept of being explicitly connected by a routable protocol

Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or....
Suggest.... Are connected to a network using a routable protocol and are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	No
Document Name	

Comment

PCA Definition – routable protocol missing.

Please clarify ESP criteria / demarcation considerations if a Reponsible Entity takes a “policy” or ruleset based approach to an ESP; in relation to PCAs. Examples involving firewall / VLans / Switch controls… Can a Responsible Entity Choose what devices are PCAs based on the policy?

The first bullet is missing the concept of being explicitly connected by a routable protocol

Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or....

Suggest

…. Are connected to a network using a routable protocol *and are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.*

Likes 0	
Dislikes 0	

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	No
Document Name	

Comment

LCRA believes the current CIP-002 SAR regarding serial-IP converters should be resolved prior to defining them as an EACMS.

Likes 0	

Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

LCRA believes the current CIP-002 SAR regarding serial-IP converters should be resolved prior to defining them as an EACMS.

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

The suggested definitions are mixing the concepts and they are making the overall understanding complicated. For example, the identification of PCA’s is done through CIP-005. CIP-002 defines the BES that defines the BCS, and at the end the BCA. It’s not written in CIP-002 that BCA need to be defined.

No where in the standard is the PCA is directly defined. The first time you see it is in part 1.1 of the R1 table in CIP-005.

For example, we have a BCA and we have a Cyber Asset they are communicating using a routable protocol, they are in the same network. Both Cyber Assets have an IP address. Theses Cyber Assets are connected via a routable protocol, thus they are in a ESP and the non qualified Cyber Asset is the PCA. In this case, the PCA is protected by an ESP.

Going with a different example, we have a BCA and we have a Cyber Asset they are communicating using a non routable protocol, there’s no network and both Cyber Asset don’t have an IP address. Those Cyber Asset are not connected via a routable protocol; thus they are not in an ESP and the non qualified Cyber Asset is nothing.

The second bullet of the PCA definition is a bit complicated, there’s the mention of “isolates routable connectivity”. We are no longer into PERMIT or DENY we are isolating, but we are still linked by the routable connectivity, ie routable protocol.

The part that is getting more confusing is the definition of the ESP. The definition of ESP has two concepts, one is based on routable protocol which works with 1.1 of CIP-005, the other is based on a logical boundary defined by one or more Electronic Access Points (EAP). What is a logical boundary ? Is a logical boundary based on routable protocol? To add to the confusion the EAP is a policy enforcement interface and it’s related to an EACMS. Is a policy a ruled based on routable protocol? Which requirement is asking to document this policy? Is it CIP-005R1.2? How to we evaluate the policy ?

Regarding the EACMS definition, which is again build with two concepts. One of the concept is “, including those not protected by an Electronic

Security Perimeter used by the responsible entity to convert routable protocol communications to non routable communications to a BCS". Considering how the current proposed standard is written, a converter (routable protocol communications to non routable communications) is associated to IRA. And IRA is associated to the concept of Intermediate System, and Intermediate System is tag as an EACMS. This logic is establish with the current proposed standard. What is the added value to add this concept to the definition of EACMS ?

Overall it seems that the SDT tried to answer multiple objectives (concepts) with the same term/definition. The end result is that we have variations in the definition and the terms are cascading. The SDT should make the definition simpler and limit the number of cascades (ESP->EAP->EACMS) . Definitions are there to ease the understanding or support the requirements, they shouldn't add additional controls.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AEPC has signed on to ACES comments:

ACES feels the way the definition of Electronic Access Point (EAP) is written in this draft is overly wordy. ACES suggests:

"An electronic policy enforcement point or a Cyber Asset interface on Electronic Access Control or Monitoring Systems that controls routable communication to and from BES Cyber Systems."

ACES feels the way the definition of Intermediate System is written in this draft is overly wordy. ACES suggests:

"Electronic Access Control or Monitoring Systems (EACMS) used to restrict Interactive Remote Access to only authorized users"

ACES also noted that the definition of an Intermidiate System no longer states that it must not be located inside an ESP, combined with the removal of the language from R2.1: "such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset." Without those two statements IRA could be initiated through an ESP to an Intermediate System located in an ESP. ACES feels the removal of the language from the definition and requirement is not what was intended and needs to be added back to ensure the security of IRA. Furthermore

with the removal of the language, it allows a Cyber Asset IRA client to connect directly to Applicable Systems, if the Intermediate System is also an EACMS with an EAP. In this scenario the Cyber Asset client connects to the EACMS using a VPN client and Multi Factor Authentication. Once connected to the Intermediate System, the IRA Client could connect directly to applicable systems. There are other scenarios, but this is the most obvious.

EACMS is already plural. so adding "one or more" to the definition of Intermediate System is redundant.

ACES feels the second bullet point on the new Management Interface should be scoped down. There are a variety of vulnerabilities in "autonomous subsystems" in which one could gain access to a system's console. Changing the scope of the definition to be ONLY those devices specifically designed and or used to allow access to a console would reduce scope creep. ACES suggests:

"Is an autonomous subsystem, specifically designed and or used to provide access to the console independently of the Cyber Asset's CPU, firmware,

and operating system;”	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	

HQ supports NPCC RSC comments and provides the following additional comments:

The suggested definitions are mixing the concepts and they are making the overall understanding complicated. For example, the identification of PCA’s is done through CIP-005. CIP-002 defines the BES that defines the BCS, and at the end the BCA. It’s not written in CIP-002 that BCA need to be defined.

No where in the standard is the PCA is directly defined. The first time you see it is in part 1.1 of the R1 table in CIP-005.

For example, we have a BCA and we have a Cyber Asset they are communicating using a routable protocol, they are in the same network. Both Cyber Assets have an IP address. Theses Cyber Assets are connected via a routable protocol, thus they are in a ESP and the non qualified Cyber Asset is the PCA. In this case, the PCA is protected by an ESP.

Going with a different example, we have a BCA and we have a Cyber Asset they are communicating using a non routable protocol, there’s no network and both Cyber Asset don’t have an IP address. Those Cyber Asset are not connected via a routable protocol; thus they are not in an ESP and the non qualified Cyber Asset is nothing.

The second bullet of the PCA definition is a bit complicated, there’s the mention of “isolates routable connectivity”. We are no longer into PERMIT or DENY we are isolating, but we are still linked by the routable connectivity, ie routable protocol.

The part that is getting more confusing is the definition of the ESP. The definition of ESP has two concepts, one is based on routable protocol which works with 1.1 of CIP-005, the other is based on a logical boundary defined by one or more Electronic Access Points (EAP). What is a logical boundary ? Is a logical boundary based on routable protocol? To add to the confusion the EAP is a policy enforcement interface and it’s related to an EACMS. Is a policy a ruled based on routable protocol? Which requirement is asking to document this policy? Is it CIP-005R1.2? How to we evaluate the policy ?

Regarding the EACMS definition, which is again build with two concepts. One of the concept is “, including those not protected by an Electronic Security Perimeter used by the responsible entity to convert routable protocol communications to non routable communications to a BCS”. Considering how the current proposed standard is written, a converter (routable protocol communications to non routable communications) is associated to IRA. And IRA is associated to the concept of Intermediate System, and Intermediate System is tag as an EACMS. This logic is establish with the current proposed standard. What is the added value to add this concept to the definition of EACMS ?

Overall it seems that the SDT tried to answer multiple objectives (concepts) with the same term/definition. The end result is that we have variations in the definition and the terms are cascading. The SDT should make the definition simpler and limit the number of cascades (ESP->EAP->EACMS) . Definitions are there to ease the understanding or support the requirements, they shouldn’t add additional controls.

Likes 0	
Dislikes 0	

Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA recommends the following edits: Cyber System should say "Two or more Cyber Assets...." as the word system implies multiples devices working together. The proposed Intermediate System definition removed the requirement of not being inside the ESP, however in the proposed language for CIP-005-8 R2.7 it states "...communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP", which implies that it must reside outside of the ESP. NCPA suggests keeping the original language in the Intermediate System to include not being located within an ESP.	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
SCI is superfluous considering that existing classification definitions can be applied. SCI does not clearly state what devices would be included and which are not included. Cyber Systems definition seems to rope in non-CIP assets. BES Cyber Systems definition is sufficient for grouping together Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	

MPC supports comments submitted by ACES.

Likes 0

Dislikes 0

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

The definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and/or domain policy server).

Also, the definition of BES Cyber Asset (BCA) uses the Glossary Term "Reliable Operations". This definition of BCA could increase the scope of the Cyber Assets being used for the operation of the BES since Reliable Operations defines Bulk-Power System's method of operation (which is a broader less precise term than BES).

Lastly the use of the term "Management Interface" needs clarification with use case and pertinent examples.

Likes 0

Dislikes 0

Response

Micah Runner - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

Black Hills Corporation has the following comments regarding the CIP definition changes:

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like:

“Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices.

(Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.)”

EAP: The definition should be revised to include the following commas to ensure clarity of the definition: “An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES

Cyber Systems or their associated Protected Cyber Assets.”

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt

Answer	No
Document Name	

Comment

Black Hills Corporation has the following comments regarding the CIP definition changes:

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like:

“Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices.

(Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.)”

EAP: The definition should be revised to include the following commas to ensure clarity of the definition: “An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.”

Likes 0	
Dislikes 0	

Response

Josh Combs - Black Hills Corporation - 3

Answer	No
Document Name	

Comment

Black Hills Corporation has the following comments regarding the CIP definition changes:

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like:

“Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices.

(Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of

Cyber Assets.)"

EAP: The definition should be revised to include the following commas to ensure clarity of the definition: "An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets."

Likes 0	
Dislikes 0	

Response

Sheila Suurmeier - Black Hills Corporation - 5

Answer	No
Document Name	

Comment

Black Hills Corporation has the following comments regarding the CIP definition changes:

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like:

"Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices.

(Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.)"

EAP: The definition should be revised to include the following commas to ensure clarity of the definition: "An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets."

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	No
Document Name	

Comment

The BCA definition changes include the defined term "Reliable Operation" which applies to the BPS by definition rather than just the BES. AECI supports the use of the previous "reliabile operation" undefined term as it would eliminate the risk of scope expansion to non-BES assets.

Likes 0	

Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The new Electronic Security Perimeter (ESP) definition still complicates the situation with respect to mixed-trust environments where a Responsible entity may choose to create ESPs and corresponding EAP's per individual Cyber System (zero trust paradigm). While this may be easier with standalone physical Cyber Assets – introducing SCI, VCA, virtual clusters, and virtual networking creates complexity that could allow unauthorized access if not carefully configured for applicable VM guests and virtual networks – especially if affinity controls are not strictly created and enforced. Marrying both ESP and zero-trust within an overall ESP would better serve our Responsible Entities and create a more secure environment as zero-trust Cyber Assets would not be directly internet-facing. Maintaining the ESP, and fully incorporating virtualization and zero trust paradigms within an identified ESP allows Responsible Entities to leverage another layer of defense (defense-in-depth) for Applicable Systems by limiting ingress/egress points and access to these BCS.

For the Shared Cyber Infrastructure definition, where is this to be identified and categorized? CIP-002 only requires the identification of BCS while the associated Technical Rationale warns of Assets with Multiple Classifications regarding high water marking. Is the entity to assume SCI must be included in CIP-002 even though it is not specifically included in the BCS definition?

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC have the following comments regarding the CIP definition changes:

Cyber Assets: The last two sentence of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like:

“Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices.

(Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of

Cyber Assets.)”

Cyber System: The definition should be changed to the following: “Two or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure working together to provide or perform a specific function.”

EAP: The definition should be revised to include the following commas to ensure clarity of the definition: “An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.”

BCA: The proposed BES Cyber Asset (BCA) definition now capitalizes “Reliable Operation”, which describes/ defines how to operate the **Bulk Electric System (BES)**. However, Reliable Operations specifically refers to the **Bulk-Power System** in its definition:

*“Operating the elements of the **[Bulk-Power System]** within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.”*

The Bulk-Power System is defined as:

“(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

(B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. (Note that the terms “Bulk-Power System” or “Bulk Power System” shall have the same meaning.)”

The Bulk-Power System term is broader in scope and less precise than the Bulk Electric System term. The Bulk Electric System is defined as:

“...all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy...”

With the capitalization of “Reliable Operations”, it could be interpreted that the proposed definition of BCA could increase the scope of the Cyber Assets used for operating the BES since Reliable Operations describes/defines how to operate the Bulk-Power System, which is a broader less precise term than BES.

SMUD and BANC would like to understand why the defined term, Reliable Operation, was used and if the intent of the revision is to broaden the scope of Cyber Assets.

Likes 0	
Dislikes 0	

Response

Tracy MacNicoll - Utility Services, Inc. - 4

Answer	Yes
Document Name	

Comment

USV support the comments made by NPCC RSC.

The proposed ESP definition uses the terms “border” and “boundary”. It is unclear what difference is between these two terms and how this difference impacts the proposed definition.

Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
In the CIP Senior Manager definition, the words "cyber security" should be deleted. As proposed it implies that the CSM is no longer responsible for physical security Standards CIP-006 & CIP-014.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the changes to definitions within draft 5.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	

Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the changes made to the definitions as posted in this Draft 5 posting.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the definition changes.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees and supports the changes to the definitions in Draft 5.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes

Document Name	
Comment	
The work the standard drafting team has done to move requirements out of the definitions and in to the standards improves the reliability standards overall.	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE supports the ISO/RTO Council comments in this area.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA has two recommendations: Cyber Asset definition: recommend improving the grammar by rewriting so there is not an “excluding” phrase separated from an “including” phrase by nothing but a comma. As written it will cause confusion. ERC definition: Given that the EAP definition would be modified to refer to EACMS as the ‘location’ of the EAP, the definition of ERC might read better if it stated “through an EAP” or “through its EACMS” rather than "through its ESP.”	
Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

FirstEnergy does not opposed the other definitions.

Likes 0	
Dislikes 0	

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

3. The SDT revised CIP-005 R1 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC disagree with the new definitions for IRA and Cyber System as the proposed definition changes may expand the scope of CIP-005, Requirement R1 to non-BES Cyber Systems.

Likes 1	Central Hudson Gas &amp; Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

As with Draft 4, BPA does not support the expansion of R1, Part 1.6 to include the protection of data traversing communications links. Expansion to communications links does not consider devices that cannot meet this criterion. Putting communication links in scope would increase costs and maintenance activities and would require re-architecture of links.

BPA does support the replacement of “protect” with “permit” in R 1 Part 1.3; this adds clarity to the intent of the requirement.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

The STD proposed a change to specify EAP as applicable systems. BC Hydro recommends providing additional clarity on evidence expectations where network-like evidence is expected at the BCS level.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF) and ACES.	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA does not agree based on comments made in question 1 related to the proposed IRA definition change.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	

HQ supports NPCC RSC comments and provides the following additional comments:

R1.2 We support the following modification “excluding time sensitive communications of Protection Systems” (replacing “communications using protocol IEC TR 61850-90-5 R-GOOSE”) assuming that the intentof the SDT was to link with the definition of Protection System (Glossary of terms)

In the column Measures, the SDT mentions VLAN and VXLAN, they are not routable protocoles. Please refer to the OSI model.

R1.3 The objective of Requirement R1.2 is to protect the BCA and the PCA through the management of the routable protocol communications (Permit/Deny). The EACMS and SCI assist in the delivery of the BCA/PCA functionalities. The EACMS and SCI Management interface are just as important, we suggest wording the requirement R1.2 and R1.3 the same way. R1.2 could be worded as: “Protect Applicable System by implementing policy enforcement to permit only needed network accessibility documenting the reason, and deny all other communications, through the ESP.” Doing so would removed the need of R1.3 or would be more “inline”.

Please note the usage of the word policy, this usage is to ensure a logical link between the requirements and the definitions.

The definition of ESP brings the concept of routable protocol and the concept of logical boundary.

R1.4 This requirement should consider including the introduction of Management interface concept. Management interface is another mean to interact with the Cyber Asset and should be address.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AEPC has signed on to ACES comments:

ACES feels R1.3 should be reworded:

“EACMS, and their supporting SCI, that control access to and from an ESP for an Applicable System in Part 1.1”

ACES feels in R1.4: “if any” is not necessary.

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer	No

Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

R1.2 We support the following modification “excluding time sensitive communications of Protection Systems” (replacing “communications using protocol IEC TR 61850-90-5 R-GOOSE”) assuming that the intentof the SDT was to link with the definition of Protection System (Glossary of terms)

In the column Measures, the SDT mentions VLAN and VXLAN, they are not routable protocoles. Please refer to the OSI model.

R1.3 The objective of Requirement R1.2 is to protect the BCA and the PCA through the management of the routable protocol communications (Permit/Deny). The EACMS and SCI assist in the delivery of the BCA/PCA functionalities. The EACMS and SCI Management interface are just as important, we suggest wording the requirement R1.2 and R1.3 the same way. R1.2 could be worded as: “Protect Applicable System by implementing policy enforcement to permit only needed network accessibility documenting the reason, and deny all other communications, through the ESP.” Doing so would removed the need of R1.3 or would be more “inline”.

Please note the usage of the word policy, this usage is to ensure a logical link between the requirements and the definitions.

The definition of ESP brings the concept of routable protocol and the concept of logical boundary.

R1.4 This requirement should consider including the introduction of Management interface concept. Management interface is another mean to interact with the Cyber Asset and should be address.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	No
Document Name	

Comment

1.3 broaden from *network accessibility* to be more objective = “*protect configuration”* in order to allow other methods to protect the configuration

Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.

Suggest

Implement methods to protect ESP and SCI configurations at Management Interfaces of Applicable Systems, per system capability, per system capability.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments.

1.3 broaden from network accessibility to be more objective = “protect configuration” in order to allow other methods to protect the configuration
Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.
Suggest
Implement methods to protect ESP and SCI configurations at Management Interfaces of Applicable Systems, per system capability, per system capability.

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1,3

Answer	No
Document Name	

Comment

Part 1.5 -> Suggestion to consider IPS/IDS on the edge of a facility instead of between discrete ESPs (E.g. if a facility has a number of ESP and non-ESP network segments, but has IPS/IDS controls at the routing edge of the facility)

Part 2.6 -> Use wording from CIP-007 that explicitly excludes storage resources (consistency in language)

Part 2.7 -> It could be clearer if this requirement just explicitly states that the intermediate system is required to be outside of the ESP that it is providing access to. The requirement to route through an EAP is then covered by R1.2 and not needed to re-stated in this requirement.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

As we did in 2022, NST objects to the use of the phrase "through the ESP," as in, "Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP;..." (R1.2). Data packets don't go "through" an ESP, they go into or out of an ESP through an access point.

NST also notes that while R1.3 requires a Responsible Entity to control network access to the Management Interfaces of SCI, there is no comparable requirement for devices (e.g., Hypervisors) that are not SCI according to the SDT's proposed definition but that still host virtual machines that are in scope for R1. This inconsistency should be addressed.

Likes 1	Central Hudson Gas &amp; Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC

Answer	No
Document Name	

Comment

1.3 broaden from network accessibility to be more objective = “protect configuration” in order to allow other methods to protect the configuration
Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.
Suggest
Implement methods to protect ESP and SCI configurations at Management Interfaces of Applicable Systems, per system capability, per system capability.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

No, due to lack of understanding of scope of impact to our systems. Better understanding of ‘applicable systems’ is needed. Provide examples.
Implementation plan guidance needed to better understand how to be in compliance.

Likes 0	

Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
ACES feels R1.3 should be reworded: “EACMS, and their supporting SCI, that control access to and from an ESP for an Applicable System in Part 1.1” ACES feels in R1.4: “if any” is not necessary.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy does not opposed these changes.	
Likes 0	

Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE supports the ISO/RTO Council comments in this area.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The standard drafting team has done an excellent job in addressing comments in CIP-005 and compliance to the new wording is backwards compatible. Manitoba Hydro notes that the definition of Intermediate System was updated to remove the phrase “The Intermediate System must not be located inside the Electronic Security Perimeter” and requirement R2.7 was added requiring “Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.”. The new requirement does not make it clear that an EACMS that contains an EAP cannot also be the intermediate system. The following wording is suggested to clarify that a separate system such as a "jump host" must be used as an Intermediate System: “Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an EAP in a separate Cyber Asset or Virtual Cyber Asset.”	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

While we can agree with the changes as they stand, should circumstances arise where additional changes to CIP-005 are necessary, we offer the following recommendations:

Part 1.3 - We recommend against the changing of "to and from" to simply "to". Controlling outbound communication is vital protection to prevent connectivity of a compromised system out to a comand-and-control server.

Part 2.3 - Consider the scenario of low impact SCI as the initiating system. The requirement phrase "Cyber Asset or Virtual Cyber Asset" excludes SCI from the set of possible initiating systems. We recommend updating the language to encapsulate all forms by using the defined term "Cyber Systems" or adding SCI.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	Yes
Document Name	

Comment

NEE supports EEI comments

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern agrees and supports the changes to the Applicable Systems, Requirements, and Measures in CIP-005 R1.

Likes 0	
Dislikes 0	

Response

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to CIP-005 Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
The standard drafting team has done an excellent job in addressing comments in CIP-005. The NSRF notes that the definition of Intermediate System was updated to remove the phrase “The Intermediate System must not be located inside the Electronic Security Perimeter” and requirement R2.7 was added requiring “Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.”. The new requirement does not make it clear that an EACMS that contains an EAP cannot also be the intermediate system. The following wording is suggested: “Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an EAP in a separate Cyber Asset or Virtual Cyber Asset.”	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	

Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the changes made to CIP-005, Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
USV supports the comments made by NPCC RSC The R1.5 requirement language limits the scope of this requirement to “routable communication entering or leaving an ESP”. Suggest moving this scoping language to the applicability column by adding “with ERC” to both high and medium impact BCS listed.	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

4. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT joins the comments submitted by the ISO/RTO Council (IRC) Standards Review Committee (SRC) and adopts them as its own.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST believes R1.3 needs to be re-worded to make it clear it applies to SCI hosting both high and medium impact BES Cyber Systems if a Responsible Entity doesn't want "high water marking" to compel treating the medium impact BCS as PCAs associated with the high impact BCS.

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1,3

Answer	No
Document Name	

Comment

Part R1.3 -> The requirement outlines controls/evidence recommended for non-BCS VCAs sharing SCI, but does not provide options potential options of classifying/securing non-BCS VCAs where physical/logical isolation cannot be achieved or is finacially restrictive.

Likes 0	

Dislikes 0

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer No

Document Name

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

R1.1 The requirement “Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. “ This requirement is ambiguous and the column measure is still referencing logical ports. Furthermore, how will this requirement will be evaluated ? The previous version of this requirement was less ambiguous.

R1.3 the definition of SCI includes the storage resource but this requirement exclude the storage resources. How is the shared storage resources managed ? What about the shared network resource ?

For some requirements the TFE was removed for “per system capability.”We do understand that TFE process isn’t optimal but it permitted more nuance than per system capability. For example, the TFE basis for approval of a technical feasibility exception are, at least the two following points;

{C}(i) is not technically possible or is precluded by technical limitations; or

{C}(ii) is operationally infeasible or could adversely affect reliability of the Bulk Electric System to an extent that outweighs the reliability benefits of Strict Compliance with the Applicable Requirement;

Per system capability is only equal to the first point but doesn’t equal to the second or to the other three. The SDT should define per system capability.

Likes 0

Dislikes 0

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1

Answer No

Document Name

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

R1.1 The requirement “Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. “ This requirement is ambiguous and the column measure is still referencing logical ports. Furthermore, how will this requirement will be evaluated ? The previous version of this requirement was less ambiguous.

R1.3 the definition of SCI includes the storage resource but this requirement exclude the storage resources. How is the shared storage resources managed ? What about the shared network resource ?

For some requirements the TFE was removed for “per system capability.”We do understand that TFE process isn’t optimal but it permitted more nuance than per system capability. For example, the TFE basis for approval of a technical feasibility exception are, at least the two following points;

(i) is not technically possible or is precluded by technical limitations; or

(ii) is operationally infeasible or could adversely affect reliability of the Bulk Electric System to an extent that outweighs the reliability benefits of Strict Compliance with the Applicable Requirement;

Per system capability is only equal to the first point but doesn’t equal to the second or to the other three. The SDT should define per system capability.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

SCI is superfluous considering that existing classification definitions can be applied. SCI does not clearly state what devices would be included and which are not included. Cyber Systems definition seems to rope in non-CIP assets. BES Cyber Systems definition is sufficient for grouping together Cyber Assets.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer	No
Document Name	

Comment

The ISO/RTO Council (IRC) Standards Review Committee (SRC) requests clarification of the term “network accessibility” used within requirement R1 Part1.1, which reads as follows: “Disable or prevent unneeded routable protocol **network accessibility** on each Applicable System, per system capability.” One of the measures also references this term: “Identity or process based access policy or workload configuration demonstrating needed **network accessibility**.” Specifically, the SRC requests that the drafting team clarify whether entities will need to define the term “network accessibility” in their documented processes or whether a standardized definition will apply. If there is a specific definition that entities are intended to use, the SRC requests that the SDT provide the definition that will apply.

Likes 0	

Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD and BANC appreciate the Standard Drafting Team's work to modify CIP-007. However, we note that the word "system" is used inconsistently, especially with regards to "per system capability", and this makes the High and Medium impact requirements less stringent than the requirements for Low impact. We recommend changing the language to "per Cyber Asset capability."	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren would like clarity on the change from where technically feasible to per system capability. Does this mean that the TFE process is going away or are they changing it to a different name?	
Likes 0	

Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the changes made to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	Yes
Document Name	
Comment	
Southern agrees and supports the changes made to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
BC Hydro agrees with the changes however seeks further clarification as follows. BC Hydro seeks clarification with use cases or examples on proposed changes to CIP-007 R1.1, whether, “per system capability” means entities are compelled to install software (if possible) that can be used to block network accessibility? Specifically, if a Cyber Asset uses a method (e.g.: host firewall) that can block the unneeded network accessibility, but that method has been determined to be detrimental to reliable operations, does this mean entities are compelled to continue to use that method although it affects the operation? BC Hydro also seeks clarification on Routable protocol network accessibility particularly, as Technical Feasibility Exception (TFE) is replaced by "per system capability", are the entities expected to make decisions on whether to document or not to document exceptions on per system capability? Please provide some use case examples and further guidance.	
Likes 0	
Dislikes 0	

Response

Micah Runner - Black Hills Corporation - 1

Answer	Yes
Document Name	

Comment

Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt

Answer	Yes
Document Name	

Comment

Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.

Likes 0	
Dislikes 0	

Response

Josh Combs - Black Hills Corporation - 3

Answer	Yes
Document Name	

Comment

Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are

within an ESP, and VCAs that are not within an ESP.	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA notes that implementation of and documenting compliance with Part 1.1 may pose technical challenges depending on an entity's architecture or processes.	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Consider rewording R1.3 for clarity.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

FirstEnergy does not opposed these changes.

Likes 0	
Dislikes 0	

Response

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	Yes
Document Name	

Comment

CHPD agrees with the proposed changed to CIP-007 R1.3.

We would also like to express our support for the decision to remove the Electronic Access Control and Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) from the list of applicable systems in CIP-007 R1.3. This change is a positive step forward, as it helps support backward compatibility with the standard.

However, in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.

We believe this reworded requirement maintains the original intent of the section while making it more straightforward and easier to understand. By replacing "VCAs that are, or are associated with, a medium or high impact BCS" with "VCAs that are within an ESP," we simplify the language while preserving the core security objectives of the requirement.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

5. The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

James Keele - Entergy - 1,3,6

Answer	No
Document Name	

Comment

Entergy disagrees with CIP-010 R1.1 as written for two reasons.

First, the requirements as written is difficult to follow as a single sentence with many oxford commas and could benefit from a rewrite to reduce confusion. Entergy proposes the requirement be rewritten similar to the following:
“Authorize changes that affect Applicable Systems and alter the behavior of one or more cyber security controls (as defined by the Responsible Entity) that serve one or more requirement parts in CIP-005 or CIP-007. This excludes procedural and physical controls.”
Secondly, Entergy is concerned regarding the removal of the previous CIP-010 R1.4 language that allowed an assessment of potentially impacted security controls, the ambiguity of the “as defined by the Responsible Entity” language, and how this could expand the scope of testing and change authorization.
As written the standard implies that any potential change to a control “defined by the Responsible Entity” would require authorization and subsequent testing, which would result in Responsible Entity security controls testing expanding from a list of potentially impacted security controls to a verification of all security controls regardless on the actual nature of the change to prove a control wasn’t impacted. As written the “defined by the Responsible Entity” could be interpreted as being related to the defining of the controls, not the defining by the Responsible Entity of a change to a control.
Entergy believes the intent of this requirement is still to perform authorizations and testing of potential and identified impacts to CIP-005 and CIP-007 controls prior to deployment. This is supported by the proposed CIP-010 R1.4 language to “verify the behavior(s) of the altered cyber security controls” which implies a verification of a pre-determined set of impacts, not a verification of ***all*** controls.
If Entergy is interpreting this correctly, then Entergy proposes that CIP-010 R1.1 be rewritten to something similar to the following, which replaces “defined” with “determined”:
“Authorize changes that the Reponsible Entity determines will affect Applicable Systems and alter the behavior of one or more cyber security controls that serve one or more requirement parts in CIP-005 or CIP-007. This excludes procedural and physical controls.”

Likes 0	
Dislikes 0	

Response

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	No
Document Name	

Comment

The problem with the current standard verbiage is that there is no requirement for a baseline, but there is no way to accomplish what the standard requires without creating baselines to monitor. Knowing you are going to be making a change that affects the baseline is a much more straightforward measure than trying to predict which/if any changes will affect CIP-005 or CIP-007 security controls tests and to what extent these should be re-tested after a change that may or may not affect the test results. For example in R1.2 the measure to include evidence such as "…a list of differences between the production and test environments with descriptions of how any differences were accounted for" cannot be accomplished without a baseline to compare against.

R2.1's requirement is unclear whether we should be monitoring for different test results, or if we should be monitoring for changes to a baseline (again, there is no mention of baselines so I'm not convinced this is a valid interpretation). If it is the case that we need to test all CIP-005 and CIP-007 controls (except physical and procedural), these are the bulk of bookending tasks for any new system. Performing this for hundreds of devices monthly is not feasible. We are a smaller entity, and we can't imagine how a larger entity could perform hundreds or thousands of bookends every month.

In Attachment 2 Section 2.1 there are two instances of the same typo for "..Responsible Entity **that that** document.."

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC do not agree with the changes to CIP-010 for the following reasons:

- CIP-010 should be reverted to its current state with the simple addition to the “Applicable Systems column” with the newly added SCI, like how it is being done for the CIP-007 revisions, to accommodate for the addition of SCI.

- The Technical Feasibility Exception was removed and not replaced with “per system capability?” If an entity has an approved TFE for CIP-010-4 R1.5, the changes proposed in CIP-010-5 R1.2 would now be applicable to that entity with no relief. Therefore, with CIP-010-5 R1.2 the entity would now be noncompliant.

- The Technical Rational for Requirement R2 is “to keep the scope of R2 to those things for which there are an ***automated solution*** that can monitor these areas and alert entities to changes.” Additionally, “The SDT also added “***per system capability***” in recognition that not all changes in scope can be monitored on every potential in-scope Cyber System. This addition makes the requirement conditional if a system is incapable of monitoring a particular unauthorized change category.” However, there is no mention that CIP-010-5 R2 Part 2.1 is only applicable for automated solutions and no automated solutions are excluded. Is that assumed/implied/allowed with the “***per system capability***” statement? Furthermore, in the Measures it states, “Examples of evidence may include, but are not limited to, reports generated from ***automated tools or manual reviews*** along with records of investigation for any unauthorized changes that were detected.” This statement causes further confusion for which the Standard Drafting Team (SDT) should address.

- The SDT should clarify if the term “per system capability” applies to Parts 2.1.1 through 2.1.7. The language that precedes the Parts reads, “...that include ***at least one cyber security control for each of the following***:” which refutes the “per system capability” statement. Is there a way for the SDT to incorporate the “per system capability” for each sub-requirement?

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

R1-Removing baseline configuration does not change what needs to be done in practice. Entities will still need to retain a baseline configuration as evidence from which to establish the changes that were authorized.

For Part 1.1 an entity will still need to show the baseline configuration prior to the change to show required cyber security controls in CIP-005 and CIP-007 are not adversely affected.

For Part 2.1 an entity will still need to provide baseline configurations for evidence that they monitor at least once every 35 calendar days for unauthorized changes to the items listed Parts 1.1 and 1.2.

Likes 0	
Dislikes 0	

Response

John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway

Answer	No
Document Name	

Comment

ISO-NE supports the ISO/RTO Council comments in this area, which are replicated here:

ISO/RTO Council is looking for clarification regarding the R2 requirement language that is mandating specific and prescriptive security controls to be monitored for change relevant to CIP-007 standard. In particular, the proposed requirement language of "… that include at least one cyber security control for each of the following…" is the area of confusion. See underlined section within the proposed requirement language below:

"Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following:

2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility;

2.1.2. Configuration of CPU or memory sharing of VCAs on SCI;

2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.

2.1.4. Configuration of malicious code protection methods;

2.1.5. Configuration of security event logging or alerting;

2.1.6. Configuration of authentication methods; and

2.1.7. Changes to the enabled or disabled status of accounts.”

ISO/RTO Council would like for the SDT to clarify if the intent of this requirement is to monitor for changes to all of the CIP-007 controls? If this is meant to be defined by the entity, ISO-NE recommends moving the sub-bullets language to the measures section similar to R1.

ISO-NE adds the following comment:

With respect to the proposed 2.1.7 sub-requirement, changes to account access should be considered part of CIP-004 Access Management as a subject and not be administered from the CIP-007 requirements. ISO-NE recommends striking the 2.1.7 sub-requirement if the sub-requirements are retained in the proposed version of CIP-010 R2.

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

With respect to R1.4, BC Hydro seeks clarity, if evidence from a representative test system is sufficient OR if evidence from a production system(s) is also required in all cases.

Requirement R1.4 uses "behavior" which is a very open term and can be used in many ways. BC Hydro seeks clarity on this with examples or use cases to explain the scope of the word behavior.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer	No
Document Name	

Comment

The SRC requests clarification regarding the language in requirement R2 that mandates the use of specific and prescriptive security controls to be monitored for changes relevant to the CIP-007 standard. In particular, the SRC requests clarification of the proposed requirement language of “… that include at least one cyber security control for each of the following….” See the underlined section within the proposed requirement language below:

“Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in

CIP-007, as defined by the Responsible Entity; **that include at least one cyber security control for each of the following**:

2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility;

2.1.2. Configuration of CPU or memory sharing of VCAs on SCI;

2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.

2.1.4. Configuration of malicious code protection methods;

2.1.5. Configuration of security event logging or alerting;

2.1.6. Configuration of authentication methods; and

2.1.7. Changes to the enabled or disabled status of accounts.”

The requirements contained in the draft of CIP-007-7 have a combined total of 21 Parts, but the draft CIP-010-5 R2 language only lists seven controls (Parts 2.1.1 – 2.1.7). It is therefore unclear whether R2 is intended to require entities to monitor for changes that impact all CIP-007 controls or only for changes that impact the items listed in R2. The SRC requests that the SDT clarify this ambiguity. If the intent is for entities to determine which controls to include in their monitoring to detect changes that would impact CIP-007 protections, the SRC recommends moving the language in Parts 2.1.1 – 2.1.7 to the measures section, similar to the way the measures section associated with requirement R1 Part 1.1 is structured.

Likes 0	
Dislikes 0	

Response

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1

Answer	No
Document Name	

Comment

NIPSCO disagrees with the changes as “security controls” needs to be better scoped and defined.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO

Answer	No
Document Name	

Comment

There appears to be inconsistency in the CIP-010-5 proposed draft language for Requirements R1 (authorization) and R2 (monitoring). The draft R2 language is more prescriptive for a set of CIP-007 controls while the draft R1 language is now non-prescriptive and related to the “behavior” of CIP-005 and CIP-007 controls, which is subjective and does not align with the list of CIP-007 controls listed in the draft R2 language. In addition, the CIP-010-5 proposed draft language is unclear whether R2 is intended to require entities to monitor for changes that impact all CIP-007 controls or only for changes that impact the items listed in R2. SPP recommends keeping the currently approved requirement language of CIP-010-4, Requirements R1 and R2, as entities have already established virtualized environments that comply with CIP-010-4 today.

Likes 0	
Dislikes 0	

Response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

The proposed language removes the baseline requirements that had previously outlined specifically what needed authorization change requests and has been replaced with referencing all of CIP-005 and CIP-007 controls. As the standards evolve over time this makes is unclear and left open for interpretation of what changes an Entity must consider for authorization requests for compliance purposes vs. “best practices”.   NCPA recommends including language in 1.1 to include the specific criteria that an Entity will be held accountable to in the requirement.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1

Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

Considering the ambiguity of the controls defined in CIP-005 5 and CIP-007 the updated version of Table R1, part 1.1 deteriorates the cyber security of the cyber assets,. The Measures column contains more explicit examples than the requirement themselves. As an example, for CIP-007 the requirement is “Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.”. The column Measures of CIP-007 R1.1 contains the following :

• Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2)

• Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1)

The SDT should ensure that controls are clearly defined in CIP-005 and CIP-007 .The SDT should also ensure that the requirements are easy measurable, and limit interpretations.

The suggested version of requirement 1.3 is defining the applicability by listing the following components; the operating systems, firmware, software, or software patches In the previous version of this requirement, the applicability was 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; and 1.1.5. Any security patches applied. The SDT should evaluate if the intent, of the new version, was it to increase the scope of the requirement.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	No
Document Name	

Comment

Regarding CIP-010 R1, Texas RE continues to be concerned security obligations will be reduced by removing the reference to baseline configurations. Establishing and maintaining baseline configurations represent best practices for system hardening. Texas RE recommends adhering to NIST Special Publication 800-53 (Rev. 5), CM-2 Baseline Configuration, which states, “Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.” See also CM-7 Least Functionality, which states: Review and update the list of authorized software programs.

Regarding CIP-010 R2, Texas RE is concerned the proposed changes to CIP-010 R1 do not include a control to verify that unintended changes have not been made. For medium impact BCS this is currently captured in requirements to authorize changes and update baseline configuration documentation within 30 calendar days. Texas RE recommends adding medium impact BCS and their associated EACMS and PCA to the Applicable Systems column of CIP-010 R2 and its subpart(s). In FERC Order 706, paragraph 398 FERC states 'We agree with ISO/RTO Council that the phrase “verification that unintended changes have not been made” captures the core issue. Our concern is that some form of verification is performed to detect when unauthorized changes have been made and to identify those changes, as well as ensuring that the proper alerts are issued.'

Further, Texas RE recommends dividing CIP-010 R2 Part 2.1 into two parts for clarity:

CIP-010 R2 Part 2.1:

The Responsible Entity shall define its cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, to include at least one cyber security control from each of the following:

2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility;

2.1.2. Configuration of CPU or memory sharing of VCAs on SCI;

2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.

2.1.4. Configuration of malicious code protection methods;

2.1.5. Configuration of security event logging or alerting;

2.1.6. Configuration of authentication methods; and

2.1.7. Changes to the enabled or disabled status of accounts.

CIP-010 R2 Part 2.2:

The Responsible Entity shall implement methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls defined in Part 2.1.

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

Considering the ambiguity of the controls defined in CIP-005 5 and CIP-007 the updated version of Table R1, part 1.1 deteriorates the cyber security of the cyber assets,. The Measures column contains more explicit examples than the requirement themselves. As an example, for CIP-007 the requirement is “Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.”. The column Measures of CIP-007 R1.1 contains the following :

• Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2)

• Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1)

The SDT should ensure that controls are clearly defined in CIP-005 and CIP-007 .The SDT should also ensure that the requirements are easy measurable, and limit interpretations.

The suggested version of requirement 1.3 is defining the applicability by listing the following components; the operating systems, firmware, software, or software patches In the previous version of this requirement, the applicability was 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; and 1.1.5. Any security patches applied. The SDT should evaluate if the intent, of the new version, was it to increase the scope of the requirement.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

The new language in CIP-010 has become more complex adding to compliance risk. Additionally, CIP-010 R2 may become harder to monitor and some of the configurations required to be monitored may require new tools than the current baseline monitoring tools.

Likes 0	
Dislikes 0	

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	No
Document Name	

Comment

The new language in CIP-010 has become more complex adding to compliance risk. Additionally, CIP-010 R2 may become harder to monitor and some of the configurations required to be monitored may require new tools than the current baseline monitoring tools.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	No
Document Name	

Comment

Please clarify if the change management approach or objective is shifting from change managing a device configuration to change managing a "policy" or process approach. The confusion is if the shift of focus is from managing assets determined by CIP 2 criteria towards Responsible Entity methods / processes / "policy" based documented plan.

Example would be dealing with planned patch management (based on schedule or plan). If the patch does not impact CIP 5 or CIP 7 security controls, does change management only apply from a deviation of the patch management plan / policy?

Suggest adding the concept of intent or "intended changes" into R1.1 and R1.4, otherwise R1.4 becomes a defacto full vulnerability assessment for any change

Suggest

R1.1

Authorize intended changes that affect Applicable Systems where those intended changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.

R1.4

As a part of the intended changes authorized per Part 1.1, verify that the behavior(s) any cyber security controls that were intentionally altered, or previously assessed as potentially being altered, were not adversely affected.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee's comments.

Please clarify if the change management approach or objective is shifting from change managing a device configuration to change managing a "policy" or process approach. The confusion is if the shift of focus is from managing assets determined by CIP 2 criteria towards Responsible Entity methods / processes / "policy" based documented plan.
Example would be dealing with planned patch management (based on schedule or plan). If the patch does not impact CIP 5 or CIP 7 security controls, does change management only apply from a deviation of the patch management plan / policy?

Suggest adding the concept of intent or "intended changes" into R1.1 and R1.4, otherwise R1.4 becomes a defacto full vulnerability assessment for any change
Suggest
R1.1
Authorize intended changes that affect Applicable Systems where those intended changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.
R1.4
As a part of the intended changes authorized per Part 1.1, verify that the behavior(s) any cyber security controls that were intentionally altered, or

previously assessed as potentially being altered, were not adversely affected.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST is unpersuaded by the SDT's argument that in modern computing environments, configuration baselines are of sufficiently limited value, while also being burdensome to maintain, that they can quite reasonably be downgraded from being included in CIP-010 requirements, and instead offered as merely one possible approach to compliance. Establishing and maintaining configuration baselines are identified as key elements of any good cyber security program in several NIST publications, including recently released SP 800-82 Release 3 ("Guide to Operational Technology (OT) Security") and the one cited by the SDT in its most recent Technical Justification document. Given the long-standing enthusiasm among both FERC and NERC personnel for examining and enhancing the mapping between CIP and NIST Standards, dropping a requirement to maintain documented configuration baselines seems oddly out of step with that and other related initiatives.

Regarding R1.1, it is NST's opinion that if the proposed language was adopted, there would be no end to arguments between Responsible Entities and Regional Entity audit teams about whether compliance had been adequately demonstrated. There are many possible changes to a Cyber Asset's installed software, such as security patches for data packet handlers, that would have no impact on the behavior of CIP-005 or CIP-007 controls. Should changes of this nature be exempt from a requirement to formally authorize them? NST is also concerned that allowing Responsible Entities to define the specific CIP-005 and CIP-007 controls within the scope of R1.1 could result in significant disparities among Responsible Entities and/or Regions in how these controls are identified. NST agrees CIP requirements should be written in a manner that avoids making them overly prescriptive, but at a time when NERC is seeking to impose greater consistency on Entities' CIP-008 programs (universal "attempts to compromise" criteria), it seems counterintuitive for a drafting team to be proposing changes to CIP-010 that would, in our opinion, reduce consistency.

Regarding R2.1:

NST notes that CIP-005 controls are omitted. We presume this to have been an oversight.

NST considers the proposed list of monitored items to be reasonable, but as with R1.1, we believe that it's a mistake to limit the scope to only those changes that could impact CIP-005 or CIP-007 controls, and that allowing Entities to decide on their own what they'll monitor could lead to many and varied interpretations of what R2.1 is intended to require. For example, 2.1.3 specifies monitoring for unauthorized "Installation, removal, and update of operating system, firmware, software, and cyber security patches." As noted previously, many such changes wouldn't alter CIP-005 and/or CIP-007 controls. Would it be permissible for an Entity to not consider 2.1.3 at all unless changes to a Cyber Asset's CIP-005 and/or CIP-007 behavior is detected?

Likes 0	
Dislikes 0	

Response

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC

Answer	No
Document Name	

Comment

Please clarify if the change management approach or objective is shifting from change managing a device configuration to change managing a “policy” or process approach. The confusion is if the shift of focus is from managing assets determined by CIP 2 criteria towards Responsible Entity methods / processes / “policy” based documented plan.
Example would be dealing with planned patch management (based on schedule or plan). If the patch does not impact CIP 5 or CIP 7 security controls, does change management only apply from a deviation of the patch management plan / policy?

Suggest adding the concept of intent or “intended changes” into R1.1 and R1.4, otherwise R1.4 becomes a defacto full vulnerability assessment for any change
Suggest
R1.1
Authorize intended changes that affect Applicable Systems where those intended changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.
R1.4
As a part of the intended changes authorized per Part 1.1, verify that the behavior(s) any cyber security controls that were intentionally altered, or previously assessed as potentially being altered, were not adversely affected.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

1) With the Guidelines and Technical Basis section removed from the CIP-010-5 standard and currently nothing in the Technical Rationale or Implementation documents outlining what a CIP-010-5 R3 paper based or active vulnerability assessment should contain, does the SDT plan to add any guidance for vulnerability assessments as it relates to SCI in these aforementioned documents?

2) We need to better understand the timeline, since the 30 day timeframe is no longer listed. Also need to better understand what evidence to provide for a “baseline”, since the R1 has been changed. Remove the phrase "the behavior of".

Justification:

1) adding "the behavior of" might make the requirement not backwards compatible

2) adding "the behavior of" could give an impression to an auditor that we need to have additional detailed testing such as penetration testing of each altered control

3) this word will cause security teams to spend a lot of time needlessly testing low-value controls rather than looking for adversaries in their networks	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy does not opposed these changes.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	

Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the changes in CIP-010 regarding the updates to change management controls. They include the change behaviors as well as the excluded physical and procedural controls, serving one or more requirement parts in CIP-005 or CIP-007.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to CIP-010.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes to CIP-010.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	

Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren supports the proposed changes to CIP-010.	
Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
USV supports the comments made by NPCC RSC	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	

6. The SDT revised CIP-003. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

Kristine Martz - Amazon Web Services - 7

Answer	No
Document Name	

Comment

The inclusion of “Shared Cyber Infrastructure (SCI) that supports a low impact BCS” in the applicable systems identified in CIP-003 R2, may be confusing to Responsible Entities who only have low impact BCS because the proposed SCI definition only identifies as SCI those programmable electronic devices that host or are associated with applicable systems of different impact ratings.

First, it appears that if a Responsible Entity is using infrastructure to host only low impact VCAs, the proposed SCI definition would make CIP-003-10 R2 inapplicable to such shared infrastructure.

Second, if the Responsible Entity is using SCI to host VCAs with a low impact and another different impact rating, the proposed standard suggests that the SCI (and all of its VCAs) would need to be protected at the level applicable to the impact rating of the highest impact system(s) hosted, which would apparently subject the SCI hosting a low impact BCS to the requirements for SCI hosting medium or high impact BCS, making the requirements in CIP-003-10 R2 unnecessary or redundant.

AWS encourages the Standard Drafting Team for Project 2016-02 to develop implementation guidance, include statements in the CIP-003 Technical Rationale, or other appropriate industry supporting documents, to clarify how Responsible Entities should implement the new requirements for SCI supporting low impact BCS under CIP-003 R2 given the two issues identified above.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST believes Appendix 1 Section 2 (Physical Security Controls) should include supporting SCI, if any, for consistency with other revised CIP-003 requirements.

Likes 0	
Dislikes 0	

Response

Ben Hammer - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

The changes to CIP-003 Specifically R2 attachment 1. should be incorporated into the CIP-004, CIP-005, CIP-006, CIP-007, and CIP-010 standards, add requirements to those standards as they pertain to low impact BES Cyber systems, either to existing requirements or to new requirements. Leave CIP-003 specifically to establishing responsibility and accountability. For Section 3 part 3.1 add an and after the 1st bullet, as shown below:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS and a Cyber System(s) outside the asset containing:
    - the low impact BCS(s); or
    - the SCI that supports a low impact BCS; **and**

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

Likes 0	
Dislikes 0	

Response

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC feel that inconsistent use of the word “system”, especially with regards to “per system capability” is making the High and Medium impact requirements less stringent than the Low impact requirements. We recommend changing the language to “per Cyber Asset capability”.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	Yes

Document Name	
Comment	
CIP Virtualization Standard proposed is CIP-003-10 is not clear. Choppy jump from section 3 to section 6, need to combine. Recommend skip this version, go to or wait for CIP-003-a	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes made to CIP-003.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

The NAGF agrees with the proposed changes to CIP-003.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern agrees with and supports the proposed changes to CIP-003.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	Yes
Document Name	

Comment

NEE supports EEI comments

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

FirstEnergy does not opposed these changes.

Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	

Likes 0

Dislikes 0

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert	

Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
Answer is yes.	
Likes 0	
Dislikes 0	
Response	

7. The SDT revised the Implementation Plan to accommodate for the future enforceable date of CIP-003-9. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

The NAGF believes that NERC needs to clarify the process and time lines for reconciliation of the multiple CIP-003 Standards Under Development and CIP-003-09 before being able to answer Question 7 accurately.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

Unintended consequences of IRA definition could increase cost of physical access controls for medium impact with IRA.

Likes 0	
Dislikes 0	

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	No
Document Name	

Comment

Unintended consequences of IRA definition could increase cost of physical access controls for medium impact with IRA.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST's "No" on this question reflects our concerns about several proposed or revised definitions and about proposed changes to CIP-003, CIP-004, CIP-005, CIP-007, and CIP-010.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy does not opposed these changes.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	Yes
Document Name	

Comment

Southern agrees with the revised Implementation Plan to become effective on or about April 1, 2026 or the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority’s order approving the Revised CIP Standards and Definitions.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	Yes
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the revised Implementation plan as proposed.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	Yes
Document Name	

Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the revised implementation plan.	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
Answer is yes.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	

8. Please provide any additional comments for the SDT to consider, if desired.

Kristine Martz - Amazon Web Services - 7

Answer	
Document Name	

Comment

AWS supports the efforts of the Project 2016-02 SDT in addressing industry comments and feedback. We understand that the proposed revisions address on-premises virtualization, though we appreciate that these changes, such as the removal of Cyber Asset references directly in requirement language, could enable further consideration of cloud technology in future standards development projects.

Should these revisions not achieve industry consensus to move forward, we encourage the SDT to consider alternatives to the standards development process to achieve the outcomes set forth in the SAR including the development of ERO endorsed implementation guidance based on the many educational resources the SDT has already created to educate industry on cyber security for virtualized environments. Additionally, we encourage NERC to develop Risk-Based Compliance Monitoring and Enforcement Program (CMEP) Practice Guides to provide direction to ERO Enterprise CMEP staff on approaches to carry out compliance monitoring and enforcement activities related to virtualization, which is already widely employed across the industry and provides a number of oprtational and cost efficiencies as well as other benefits. Clear guidance on CIP compliance for virtual assets would greatly benefit the industry and its stakeholders by allowing for compliance certainty when moving towards greater virtualization.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	
Document Name	

Comment

ACES and it's members would like to thank the SDT for their continued hard work.

Likes 0	
Dislikes 0	

Response

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	
Document Name	

Comment

With the Guidelines and Technical Basis section removed from the CIP-010-5 standard and currently nothing in the Technical Rationale or Implementation documents outlining what a CIP-010-5 R3 paper based or active vulnerability assessment should contain, does the SDT plan to add any guidance for vulnerability assessments as it relates to SCI in these aforementioned documents?

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 6

Answer	
Document Name	

Comment

No additional comments at this time.

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

See comments submitted by the Edison Electric Institute

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon supports the comments submitted by the EEI.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5

Answer	
Document Name	

Comment

None at this time.

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer	
Document Name	

Comment

The SDT added this exemption 4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations. Our understanding is that “communication networks” is associated with routable protocol (layer 3 of the OSI model) and that “data communication links” is associated with non routable protocol (layer 2 of the OSI model). SDT should clarify the intend if this is not the case.

The SDT should ensure the security posture of the Cyber Assets and not only facilitating the adoption of new technology by introducing ambiguous requirements.

The SDT should evaluate the requirements against the ERT tool approach. In other words, can the requirement be evaluated with the ERT tool.

The SDT should ensure that the requirements are clear and precise and stand by themselves and that no additional reading is required, i.e., technical rational. The technical rational should be viewed as a rational and not provide explanation on how to understand the requirement.

The SDT should review the requirements with the concept of applying Protection Systems definition.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	
Document Name	

Comment

The CIP-004-8 R2.3, R4.1.2, R5.1, R5.2, R6.1.2, R6.3, exclusion ‘(except for medium impact without ERC)’ appears to be unnecessary considering medium impact without ERC is not an applicable system of the requirement.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	
Document Name	

Comment

In the draft standards there is inconsistency in the wording of section “C. Compliance | 1. Compliance Monitoring Process | 1.1. Compliance Enforcement Authority:”. The following wording is used in CIP-003-10, and is suggested for the other standards as it matches the definition in the NERC Rules of Procedures:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with mandatory and enforceable Reliability Standards.

The following is used in CIP-004-8, CIP-005-8, CIP-007-7 and CIP-010-5

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA)

means NERC or the Regional Entity, or any entity as otherwise designated by an

Applicable Governmental Authority, in their respective roles of monitoring and/or

enforcing compliance with mandatory and enforceable Reliability Standards in

their respective jurisdictions.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	
Document Name	

Comment

Thank you for the ability to comment.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1

Answer	
Document Name	

Comment

The SDT added this exemption 4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations. Our understanding is that “communication networks” is associated with routable protocol (layer 3 of the OSI model) and that “data communication links” is associated with non routable protocol (layer 2 of the OSI model). SDT should clarify the intend if this is not the case.

The SDT should ensure the security posture of the Cyber Assets and not only facilitating the adoption of new technology by introducing ambiguous requirements.

The SDT should evaluate the requirements against the ERT tool approach. In other words, can the requirement be evaluated with the ERT tool.

The SDT should ensure that the requirements are clear and precise and stand by themselves and that no additional reading is required, i.e., technical rational. The technical rational should be viewed as a rational and not provide explanation on how to understand the requirement.

The SDT should review the requirements with the concept of applying Protection Systems definition.

Likes 0

Dislikes 0

Response

Richard Vendetti - NextEra Energy - 5

Answer

Document Name

Comment

NEE supports EEI comments

Likes 0

Dislikes 0

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer

Document Name

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).

Likes 0

Dislikes 0

Response

Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy

Answer

Document Name

Comment

Duke Energy thanks the Virtualization Standard Drafting Team for their hard work to get to Draft 5, and for their careful consideration of industry comments from Draft 4.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	
Document Name	

Comment

In the draft standards there is inconsistency in the wording of section “C. Compliance | 1. Compliance Monitoring Process | 1.1. Compliance Enforcement Authority:”. The following wording is used in CIP-003-10, and is suggested for the other standards as it matches the definition in the NERC Rules of Procedures:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with mandatory and enforceable Reliability Standards.

The following is used in CIP-004-8, CIP-005-8, CIP-007-7 and CIP-010-5

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA)

means NERC or the Regional Entity, or any entity as otherwise designated by an

Applicable Governmental Authority, in their respective roles of monitoring and/or

enforcing compliance with mandatory and enforceable Reliability Standards in

their respective jurisdictions.

Likes 0	
Dislikes 0	

Response

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment	
CIP-005 R2.6: BPA reiterates disagreement with the requirement to prevent sharing of memory resources in R2.6. The theoretical risk represented by CPU-sharing is not high enough to mandate the significant re-architecture required to adequately separate CPU usage as specified in Part 2.6. BPA recommends allowing the continued use of shared resources to allow entities the flexibility to balance risk mitigation with resources, maintenance and cost of maintaining the grid.	
Likes 0	
Dislikes 0	
Response	

Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	

Comment

FirstEnergy asks the DT for clarification training requirements for CIP-004.

Training requirement 2.2 and 2.3 appear to be inconsistent in the description with the use of “includes Mediums with ERC” as well as Access Authorization/verification in requirement 4.1 and 4.2.

Likes 0	
Dislikes 0	

Response

Consideration of Comments

Project Name:	2016-02 Modifications to CIP Standards | Virtualization - Draft 5
Comment Period Start Date:	10/3/2023
Comment Period End Date:	11/29/2023
Associated Ballot(s):	2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 5 ST 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 5 ST

There were 71 sets of responses, including comments from approximately 185 different people from approximately 116 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Director, Standards Development Latrice Harkness (via email) or at (404) 858-8088.

Questions

1. The SDT modified the IRA definition, CIP-005 R2 and CIP-004 Applicable Systems to address IRA in routable to nonroutable (i.e., IP to serial) conversion scenarios. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

2. The SDT modified other (not related to IRA) definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

3. The SDT revised CIP-005 R1 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

4. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

5. The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.

6. The SDT revised CIP-003. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal.

7. The SDT revised the Implementation Plan to accommodate for the future enforceable date of CIP-003-9. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

8. Please provide any additional comments for the SDT to consider, if desired.

The Industry Segments are:

1 — Transmission Owners

2 — RTOs, ISOs

3 — Load-serving Entities

4 — Transmission-dependent Utilities

5 — Electric Generators

6 — Electricity Brokers, Aggregators, and Marketers

7 — Large Electricity End Users

8 — Small Electricity End Users

9 — Federal, State, Provincial Regulatory or other Government Entities

10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Jaimin Patal	Saskatchewan Power Corporation (SPC)	1	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Marc Gomez	Southwestern Power Administration (SWPA)	1	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy	1,3	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Company (MEC)		
					Bryan Sherrow	Board Of Public Utilities (BPU)	1	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Michael Ayotte	ITC Holdings	1	MRO
Public Utility District No. 1 of Chelan County	Anne Kronshage	6		Public Utility District No. 1 of Chelan County - Voting Group	Anne Kronshage	Public Utility District No. 1 of Chelan County	6	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Rebecca Zahler	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Nick Fogleman	Prairie Power, Inc.	1,3	SERC
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Marcus Perkins	Southern Maryland Electric Cooperative	3	RF
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Elizabeth Davis	PJM	2	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Leslie Burke	Southern Company - Southern Company Generation	5	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC
					Deidre Altobell	Con Edison	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Jeffrey Streifling	NB Power Corporation	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
					Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
					Randy Buswell	Vermont Electric Power Company	1	NPCC
					James Grant	NYISO	2	NPCC
					John Pearson	ISO New England, Inc.	2	NPCC
					Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
					Randy MacDonald	New Brunswick Power Corporation	2	NPCC
					Dermot Smyth	Con Ed - Consolidated	1	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Edison Co. of New York		
					David Burke	Orange and Rockland	3	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					David Kwan	Ontario Power Generation	4	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Sean Cavote	PSEG	4	NPCC
					Jason Chandler	Con Edison	5	NPCC
					Tracy MacNicoll	Utility Services	5	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	1	NPCC
Shannon Mickens	Shannon Mickens		MRO,SPP RE,WECC	SPP RTO	Shannon Mickens	Southwest Power Pool Inc.	2	MRO
					Mia Wilson	Southwest Power Pool Inc.	2	MRO
					Josh Phillips	Southwest Power Pool Inc.	2	MRO
					Shelly Young	Southwest Power Pool Inc.	2	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					David Minick	Southwest Power Pool Inc.	2	MRO
					Mike Wikerson	Southwest Power Pool Inc.	2	MRO
					Chris Evans	Southwest Power Pool Inc.	2	MRO
					Barry Bull	Southwest Power Pool Inc.	2	MRO
					Rebecca Sanders	Southwest Power Pool Inc.	2	MRO
					Steve Shirley	Southwest Power Pool Inc.	2	MRO
					Cheryl Kirk	Southwest Power Pool Inc.	2	MRO
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
						Electric Power Cooperative		
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. ***The SDT modified the IRA definition, CIP-005 R2 and CIP-004 Applicable Systems to address IRA in routable to nonroutable (i.e., IP to serial) conversion scenarios. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.***

Sean Steffensen - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Edited	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
James Keele - Entergy - 1,3,6	
Answer	No
Document Name	
Comment	
CIP-004-7 - R6.1.2 provisioned physical access to physical BCSI (except for BCSI at a medium impact BCS without ERC). The definition which is listed in the CIP-004-8 Technical Rationales and justification states: For BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet.	

By the NERC definition of "Physical Access" ERC does not exist. The additional language of (except for BCSI at a medium impact BCS without ERC) should be removed since a lockable file cabinet is not able to have External Routable Connectivity (ERC) making this statement mute.

The term: Interactive Remote Access (IRA) needs to be defined before it is introduced in a NERC Requirement. It is listed in the Technical Rationale, there is no definition. List the difference between IRA and ERC. If you have ERC, you have IRA. You cannot have either with "Physical Access" as defined as stated above.

Remove R6.1.2 and refer to is as access to BCSI whether it is electronic or physical. Make it simple. You either have been granted access to BCSI or you have not. For R4.1.2 it doesn't matter if the PSP has ERC or not. Access is access. By adding in ERC, it makes the entity to perform more work and create more policies that do not provide any more security. It makes the compliance piece harder to meet while not gaining any security.

Take guidance from the Nuclear Regulatory Commission (NRC) on Critical Group Membership. You either a critical group member or you are not. Critical group membership allows an individual to work on critical digital assets, whether it is physical or electronical. 1 access control for both types of access.

Medium impact BCS with IRA SCI supporting an Applicable System in this Part – this section needs more clarity on what it is asking the entity to look for. Measures would need to be added to better understand what the ask is.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The Physical BCSI reference is in relation to BCSI **"at"** a medium impact BCS without ERC, the ERC reference in relation to the medium impact BCS where the BCSI is stored, not the BCSI itself. The Parenthetical is a separate statement.

The same concept applies to R4 Part 4.1.2, where the relationship is between the BCS and ERC not the PSP and ERC.

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	No

Document Name	
Comment	

The SDT has created two different ways of scoping IRA with the current draft of the definition of IRA. In the first case, RE's determine if in-scope IRA exists within the definition, by deciding if the destination Cyber System is inside an ESP (as there are no cases where a Cyber System would be inside an ESP but would not be an Applicable System), while the second case requires RE's to first use the definition to determine if the a protocol conversion is taking place, then use the Applicable Systems of CIP-005 R2 to determine if the destination device is in-scope.

For example, in case 1: An EMS Server (high impact BCA) is inside an ESP. An engineer logs into the EMS server from a jump host outside the ESP. This access meets the first criteria of the definition IRA, and we don't need the Applicable Systems of CIP-005 R2 to determine it is in-scope because all such access would be in-scope.

Case 2: A comm server hosts telnet servers that translate IP to serial for a RTU at a remote site. A employee can initiate a telnet session to the comm server to remotely program the device. This device DOES meet the definition of IRA. But we cannot determine if it is in-scope IRA without knowing the RTU's classification. If the device is low impact or not BES, it is technically IRA, but has no requirements.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. CHPD recommends an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

CHPD's recommendation is as follows:

Definitions:

Interactive Remote Access - User-initiated, interactive electronic access by a person using a bi-directional routable protocol:

- To a routable Cyber System
- That is converted to a non-routable protocol that allows interactive access to a Cyber System

- To a Management Interface

Intermediate System - An Electronic Access Control or Monitoring System(s) that Interactive Remote Access to BES is permitted to originate from.

CIP-005 R2.1

Applicable Systems - High impact BCS and their PCA(s); Medium impact BCS and their PCA(s)

Requirement - Permit Interactive Remote Access (IRA) from outside an ESP, if any, only from an Intermediate System.

CIP-005 R2.2-R2.7 - Unchanged

Thus, all interactive remote access is "IRA", but only IRA that originates from outside an ESP to an Applicable System is in-scope of CIP-005 R2. The system-to-system exemption is no longer needed, as the access has to be "interactive" per the definition of IRA. The ESP-to-ESP exemption is also no longer needed, as that type of communication naturally falls out-of-scope of the updated R2.1 language. And the non-routable concern is brought into the fold by the second bullet point of the definition of IRA.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. While it is true that there is some scoping found within NERC Glossary definitions, is only through careful review of the definitions and Standards that a determination of scope of impact can be identified. The SDT chose to modify definitions within our SAR to remove as much scoping language from the definitions as is possible and beneficial, to enable the definition to cover as many scenarios as possible. The intent is to have scope identified through the combination of definition, applicability, and requirement language. Therefore, the scoping is developed through the same process for each bullet in the IRA definition.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	No
Document Name	

Comment

FirstEnergy suggests including the following in the proposed IRA Definition:

- User-initiated electronic access by a person using a bi-directional routable protocol:
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System **when conversion is performed by an device located outside of the ESP of the Cyber System**

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT considered the suggestion and believes that the suggestion would not address the issue in the SAR. The SDT is trying to clarify situations where there is no ESP.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC appreciate the Standard Drafting Team’s work to modify the IRA definition. In the second bullet of the proposed definition, we recommend changing the words “To a Cyber System…” to “To a BES Cyber System…” so that the scope is not expanded to non-BES, EACMS and PACS.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. While it is true that there is some scoping found within NERC Glossary definitions, is only through careful review of the definitions and Standards that a determination of scope of impact can be identified. The SDT chose to modify definitions within our SAR to remove as much scoping language from the definitions as is possible and beneficial, to enable the definition to cover as many scenarios as possible. The intent is to have scope identified through the combination of definition, applicability, and requirement language. Therefore, the scoping is developed through the same process for each bullet in the IRA definition.

Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

The gap between what is system-to-system communications and what is Interactive Remote Access (IRA) with the new IRA definition should addressed. Entities often rely on IRA ports for system-to-system communication but have not adequately enforced protections or deployed additional internal controls to ensure that malicious actors do not use the ports, or the ports are used later to establish user-initiated remote access. Additional technical measures or controls should be added to a new definition to ensure validity of declared system-to-system communications to Applicable Systems are not used for IRA. In addition, approval of CIP-005-8, with the modified IRA definition, is still conditional, based upon approval of the entire suite of proposed CIP definitions associated with virtualization and SCI terminology. With no formal definition of system-to-system, there is still lingering issues regarding where this fine line between system-to-system and IRA exists. By stipulating system-to-system communications excludes the ability for direct user-initiated electronic access at any time, better delineates IRA from system-to-system communications.

Suggested Interactive Remote Access definition:

User-initiated electronic access by a person using a bi-directional routable protocol:

To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);

That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or

To a Management Interface.

Interactive Remote Access does not include:

Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs; or System-to-system process communications that cannot be used to establish user-initiated electronic access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT feels that the language added to the end of the definition is unnecessary because it describes communication that is out of scope of the definition.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Although IP to Serial Converters are devices within a ESP and PSP environment in which they could be manipulated if the network is compromised, they can not be directly interacted with through interactive remote access. The serial based systems down stream of the converter would only operate on non-routable serial communications protocol. The language as proposed inappropriately brings these non-IRA devices into scope of this requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The v5TAG included this specific issue within the SAR to clarify how to control remote access via what was termed the “500 mile serial cable.” The SDT concurred that this was an important clarifying step to take. The systems that are being protected through these updates are the BCS themselves, not the IP to Serial Converters and the security controls are to be applied to the routable protocol side of the conversion. As such the SDT feels the changes are appropriate and necessary.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	

Answer	No
Document Name	
Comment	
Do not agree with the statement, "That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System;" When read, the wording implies that the connection must always be coverted to a non-routable protocol. A more correct statement would be, "To include connections, which are converted by the responsible entity to a non-routable protocol that allows access to a Cyber System".	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Ben Hammer - Western Area Power Administration - 1	
Answer	No
Document Name	
Comment	
The use of a non routable protocol ip to serial does not cover scenarios where an intermediate system is used first to get to the protocol converter. For example, a utility using a centralized EACMS (intermediate server) placed infront of the protocol converter that mitigates the security risks.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The identified control of an Intermediate System between the initiating Cyber Asset and the protocol converter could itself fulfill the requirement language clarified in CIP 005 R2.	

Sheila Suurmeier - Black Hills Corporation - 5	
Answer	No
Document Name	
Comment	

Black Hills Corporation requests the standards drafting team consider defining the term “system-to-system process communications” as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying “system-to-system process communications” versus IRA would allow entities to know which controls need to be applied.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

Our recommendation is as follows:

Definitions:

Interactive Remote Access -

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs; or System-to-system process communications that cannot be used to establish user-initiated electronic access.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. While it is true that there is some scoping found within NERC Glossary definitions, is only through careful review of the definitions and Standards that a determination of scope of impact can be identified. The SDT chose to modify definitions within our SAR to remove as much scoping language from the definitions as is possible and beneficial, to enable the definition to cover as many scenarios as possible. The intent is to have scope identified through the combination of definition, applicability and requirement language. Therefore, the scoping is developed through the same process for each bullet in the IRA definition. The SDT feels that the language added to the end of the definition is unnecessary because it describes communication that is out of scope of the definition.

Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt

Answer	No
Document Name	

Comment

Black Hills Corporation requests the standards drafting team consider defining the term “system-to-system process communications” as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying “system-to-system process communications” versus IRA would allow entities to know which controls need to be applied.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

Our recommendation is as follows:

Definitions:

Interactive Remote Access - User-initiated electronic access by a person using a bi-directional routable protocol: • To a Cyber System protected by an Electronic Security Perimeter(s) (ESP); • That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or • To a Management Interface. Interactive Remote Access does not include: Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or System-to-system process communications that cannot be used to establish user-initiated electronic access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. While it is true that there is some scoping found within NERC Glossary definitions, is only through careful review of the definitions and Standards that a determination of scope of impact can be identified. The SDT chose to modify definitions within our SAR to remove as much scoping language from the definitions as is possible and beneficial, to enable the definition to cover as many scenarios as possible. The intent is to have scope identified through the combination of definition, applicability, and requirement language. Therefore, the scoping is developed through the same process for each bullet in the IRA definition. The SDT feels that the language added to the end of the definition is unnecessary because it describes communication that is out of scope of the definition.	
Josh Combs - Black Hills Corporation - 3	
Answer	No
Document Name	
Comment	

Black Hills Corporation requests the standards drafting team consider defining the term “system-to-system process communications” as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying “system-to-system process communications” versus IRA would allow entities to know which controls need to be applied.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

Our recommendation is as follows:

Definitions:

Interactive Remote Access -

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs; or System-to-system process communications that cannot be used to establish user-initiated electronic access.

Likes 0	
Dislikes 0	
Response	

Thank you for your comments. While it is true that there is some scoping found within NERC Glossary definitions, is only through careful review of the definitions and Standards that a determination of scope of impact can be identified. The SDT chose to modify definitions within our SAR to remove as much scoping language from the definitions as is possible and beneficial, to enable the definition to cover as many scenarios as possible. The intent is to have scope identified through the combination of definition, applicability, and requirement language. Therefore, the scoping is developed through the same process for each bullet in the IRA definition. The SDT feels that the language added to the end of the definition is unnecessary because it describes communication that is out of scope of the definition.

Micah Runner - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

Black Hills Corporation requests the standards drafting team consider defining the term “system-to-system process communications” as it is referenced in the current and proposed definition of Interactive Remote Access (IRA). Clearly identifying “system-to-system process communications” versus IRA would allow entities to know which controls need to be applied.

The SDT should make scoping of what is in-scope and what is out-of-scope consistent between all types of IRA. We recommend an approach that classifies all remote access as IRA and only places requirements on IRA that originates from a device outside the ESP to a high or medium BCS or PCA.

Additionally, the definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or even firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and domain policy server).

Our recommendation is as follows:

Definitions:

Interactive Remote Access -

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);

- That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or - To a Management Interface. Interactive Remote Access does not include: Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or System-to-system process communications that cannot be used to establish user-initiated electronic access.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. While it is true that there is some scoping found within NERC Glossary definitions, is only through careful review of the definitions and Standards that a determination of scope of impact can be identified. The SDT chose to modify definitions within our SAR to remove as much scoping language from the definitions as is possible and beneficial, to enable the definition to cover as many scenarios as possible. The intent is to have scope identified through the combination of definition, applicability, and requirement language. Therefore, the scoping is developed through the same process for each bullet in the IRA definition. The SDT feels that the language added to the end of the definition is unnecessary because it describes communication that is out of scope of the definition.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro appreciates the opportunity to review and comment and offers the following. BC Hydro requests clarity on the definition of Interactive Remote Access (IRA) for the following reason: IRA definition (second bullet) uses the words "To a Cyber System..." which could lead to the understanding that the scope is expanded to non-BES, EACMS and PACS.	

BC Hydro proposes that the wording is changed to "To a BES Cyber System..." to make it clear.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. While it is true that there is some scoping found within NERC Glossary definitions, is only through careful review of the definitions and Standards that a determination of scope of impact can be identified. The SDT chose to modify definitions within our SAR to remove as much scoping language from the definitions as is possible and beneficial, to enable the definition to cover as many scenarios as possible. The intent is to have scope identified through the combination of definition, applicability, and requirement language. Therefore, the scoping is developed through the same process for each bullet in the IRA definition.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by ACES.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to ACES.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	

NIPSCO does not agree with the proposed definition. The new definition of IRA seems to be virtually the same as ERC. It is a distinction without much of a difference.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT notes that IRA and ERC definitions are similar, however the IRA definition includes user initiated access, IP to Serial Conversion and management interfaces. The difference is in the applicability of requirements based on the type of access.

Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO

Answer	No
Document Name	

Comment

Due to the non-routable protocol's inability to cross an EAP, the definition of Interactive Remote Access (IRA) should not apply. Given this limitation, the ability to cross an EAP to access a Cyber Asset within the ESP should have its definition limited to only routable protocols.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment	
NCPA suggests editing the new IRA definition to say "To a BCS..." in the first bullet point in lieu of just "Cyber Systems" to avoid including other system types such as EACMS, PACS and PCAs.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. While it is true that there is some scoping found within NERC Glossary definitions, is only through careful review of the definitions and Standards that a determination of scope of impact can be identified. The SDT chose to modify definitions within our SAR to remove as much scoping language from the definitions as is possible and beneficial, to enable the definition to cover as many scenarios as possible. The intent is to have scope identified through the combination of definition, applicability, and requirement language. Therefore, the scoping is developed through the same process for each bullet in the IRA definition.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
HQ supports NPCC RSC comments and provides the following additional comments: If the goal is to ensure that user interactive actions, is done remotely(i.e., not in the PSP), on a BCA and PCA, then those actions must go through an intermediate system, and the users must have training, ie CIP-004. The IRA definition should be simple and not technologically limited (routable vs nonroutable). The security risks associated to IRA are not dependent on the routable scenarios or routable to nonroutable (i.e., IP to serial) conversion scenarios. They are associated to the remote access.	

Furthermore, if the intentionof the IRA definition is to say "Communication that originates from a BCA or a PCA protected by any of the Responsible Entity's ESPs", Why is this part of the definition when CIP-005 R1.1 Requires that BCA or a PCA are to be protected by an ESP ? Also, since CIP-005 R2.4 and R2.5, include System-to-system process communication, I would remove "or System-to-system process communication." to the definition of IRA as the concept is in the requirements. SDT should simplify the definition. Suggested improvements include: IRA: User-initiated electronic access by a person to a BCA or a PCA . Interactive Remote Access does not include: Out going communication that originates from a BCA or PCA; The modifications to CIP-004 are adequate. The modification to CIP-005 R2, more precisely R2.7 is not required, since R1.2 is there to manage all the routable communication. Also R2.7 implies that the converter (IP to Serial) is outside of the ESP. [BCA] – IP – [F/W] – [IPtoSerial] - Serial	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The proposed IRA definition oversimplifies the challenge and does not address all appropriate instances of IRA. R2.7 is required in order to authenticate remote users before access into the ESP is allowed.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE agrees that IRA definitions and requirements should be modified to address IRA in routable to nonroutable conversion scenarios. Texas RE noticed however, a gap between the glossary definition and the proposed requirements as written, specifically with regards to IRA to SCI.

The SDT has defined IRA as meeting one of the three following criteria:

- User-initiated electronic access by a person using a bi-directional routable protocol to a cyber system protected by an ESP.
- User-initiated electronic access by a person using a bi-directional routable protocol that is converted by the responsible entity to a non-routable protocol that allows access to a cyber system.
- User-initiated electronic access by a person using a bi-directional routable protocol to a management interface.

In CIP-005 R2 Part 2.1 the SDT requires that IRA only be permitted through an Intermediate System. One of the applicable systems is “SCI supporting an Applicable System in this Part.” In CIP-005 R1 Part 1.1 applicable systems are required to be protected by an ESP. SCI is not an applicable system. Since SCI are not an applicable system in CIP-005 R1 Part 1.1 they are not required to be protected by an ESP. An SCI not protected by an ESP will not match the “User-initiated electronic access by a person using a bi-directional routable protocol to a cyber system protected by an ESP” criteria. As such, these communications would not meet the definition of IRA and would therefore be out of scope for CIP-005 R2 Part 2.1.

Texas RE therefore recommends modifying the proposed glossary definition of IRA to include a “User-initiated electronic access by a person using a bi-directional routable protocol to SCI supporting a BCS.”

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT feels that the security issue that SCI introduces is not through the production interfaces (since they are covered by their inclusion in the BCA, PCA etc.) but through the Management Interface to the SCI. This is the reason for the inclusion of the third bullet in the IRA definition.

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No

Document Name	

Comment

AEPC has signed on to ACES comments:

ACES feels the first sub bullet to the IRA definition is overly wordy and is confusing. ACES sugguests:

“To a BCS or a defined Electronic Access Point (EAP).”

The CIP standards are not concerened with IRA to any other systems besides Applicable Systems/BCS, so scoping the definition to just what NERC/CIP’s definition is, does not allow any scope creep.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The proposed IRA definition oversimplifies the challenge and does not address all appropriate instances of IRA. While it is true that there is some scoping found within NERC Glossary definitions, is only through careful review of the definitions and Standards that a determination of scope of impact can be identified. The SDT chose to modify definitions within our SAR to remove as much scoping language from the definitions as is possible and beneficial, to enable the definition to cover as many scenarios as possible. The intent is to have scope identified through the combination of definition, applicability, and requirement language. Therefore, the scoping is developed through the same process for each bullet in the IRA definition.

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:
If the goal is to ensure that user interactive actions, is done remotely(i.e., not in the PSP), on a BCA and PCA, then those actions must go through an intermediate system, and the users must have training, ie CIP-004.

The IRA definition should be simple and not technologically limited (routable vs nonroutable).
The security risks associated to IRA are not dependent on the routable scenarios or routable to nonroutable (i.e., IP to serial) conversion scenarios. They are associated to the remote access.
Furthermore, if the intentionof the IRA definition is to say “Communication that originates from a BCA or a PCA protected by any of the Responsible Entity’s ESPs”, Why is this part of the definition when CIP-005 R1.1 Requires that BCA or a PCA are to be protected by an ESP ?
Also, since CIP-005 R2.4 and R2.5, include System-to-system process communication, I would remove “or System-to-system process communication.” to the definition of IRA as the concept is in the requirements.
SDT should simplify the definition. Suggested improvements include:

- IRA: User-initiated electronic access by a person to a BCA or a PCA .
- Interactive Remote Access does not include: Out going communication that originates from a BCA or PCA;

The modifications to CIP-004 are adequate.
The modification to CIP-005 R2, more precisely R2.7 is not required, since R1.2 is there to manage all the routable communication. Also R2.7 implies that the converter (IP to Serial) is outside of the ESP. [BCA] – IP – [F/W] – [IPtoSerial] - Serial

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The proposed IRA definition oversimplifies the challenge and does not address all appropriate instances of IRA. R2.7 is required in order to authenticate remote users before access into the ESP is allowed.

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

By adding the new applicable system of medium impact with IRA in CIP-004 it causes confusion. LCRA believes the intent is to require training and background checks only for individuals with provisioned electronic access to medium impact BCS with IRA; however, it could be construed that any access to these devices requires R2 and R3 to be complied with.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The intent of the inclusion of Medium impact BCS with IRA within the bulk of CIP-004 is to ensure those requirements are met just as others are where the security risk includes remote access. The exclusion of medium impact BCS without ERC is a nod to backwards compatibility and the concern that many of the CIP-004 Requirements have a time restriction that may not be able to be served if the disabling of access requires a drive to the location.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
By adding the new applicable system of medium impact with IRA in CIP-004 it causes confusion. LCRA believes the intent is to require training and background checks only for individuals with provisioned electronic access to medium impact BCS with IRA; however, it could be construed that any access to these devices requires R2 and R3 to be complied with.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The intent of the inclusion of Medium impact BCS with IRA within the bulk of CIP-004 is to ensure those requirements are met just as others are where the security risk includes remote access. The exclusion of medium impact BCS without ERC is a nod to backwards compatibility and the concern that many of the CIP-004 Requirements have a time restriction that may not be able to be served if the disabling of access requires a drive to the location.	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	No
Document Name	

Comment

There seems to be an inconsistency between EACMS definition and the CIP-005 R2 requirements:

1) {C}EACMS definition includes a protocol converter for BCS where no ESP exists.

2) New R2 Applicable Systems requires an Intermediate System

3) New R2.7 requires an ESP between the Intermediate System and the BCS

Is the intent of the SDT to require the protocol converter to be an Intermediate System? In the case where no ESP exists, then R2.7 cannot be met.

Suggest change the Applicable Systems in R2.1 to exclude situations without ERC or change R2.7 requirements to exclude situations where protocol converter is used and there is no ESP

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT believes that the definitions and requirement language is consistent as intended.

1. EACMS definition includes a protocol converter for BCS where no ESP exists. True, and only for “those” that perform electronic access control or electronic access monitoring for the BCS (OR ESP).
2. Applicable Systems columns only define where a requirement is applicable. They do not establish a requirement in themselves. If no Intermediate Systems are in use, then there is no applicability. However, if there is IRA, then there may be an issue with compliance to R2 Part 2.1.

3. R2 Part 2.7 requires the IS to be placed such that “routable protocol communications” to the BCS must go through an ESP. This does not require an ESP unless there is routable protocol communications between the IS and BCA. Due to the “routable protocol communications” CIP-005 R1 would be applicable, and there should already be an ESP.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments.

There seems to be an inconsistency between EACMS definition and the CIP-005 R2 requirements:
1) EACMS definition includes a protocol converter for BCS where no ESP exists.
2) New R2 Applicable Systems requires an Intermediate System
3) New R2.7 requires an ESP between the Intermediate System and the BCS
Is the intent of the SDT to require the protocol converter to be an Intermediate System? In the case where no ESP exists, then R2.7 cannot be met.
Suggest change the Applicable Systems in R2.1 to exclude situations without ERC or change R2.7 requirements to exclude situations where protocol converter is used and there is no ESP

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT believes that the definitions and requirement language is consistent as intended.

1. EACMS definition includes a protocol converter for BCS where no ESP exists. True, and only for “those” that perform electronic access control or electronic access monitoring for the BCS (OR ESP).
2. Applicable Systems columns only define where a requirement is applicable. They do not establish a requirement in themselves. If no Intermediate Systems are in use, then there is no applicability. However, if there is IRA, then there may be an issue with compliance to R2 Part 2.1.

3. R2 Part 2.7 requires the IS to be placed such that “routable protocol communications” to the BCS must go through an ESP. This does not require an ESP unless there is routable protocol communications between the IS and BCA. Due to the “routable protocol communications” CIP-005 R1 would be applicable, and there should already be an ESP.

Alain Mukama - Hydro One Networks, Inc. - 1,3

Answer	No
Document Name	

Comment

There is a conflict between the newly proposed EACMS which includes "those not protected by an Electronic Security Perimeter used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS" and CIP-005-8 R2.7 that mandates ESP between Intermediate System and High/Medium Impact BCS. Please clarify how to identify ESP when protocol converter is used to connect High/Medium Impact Cyber System serially for IRA from Intermediate System. {C}{C}

Likes 0	
Dislikes 0	

Response

Thank you for your comments. R2 Part 2.7 requires the IS to be placed such that “routable protocol communications” to the BCS must go through an ESP. This does not require an ESP unless there are routable protocol communications between the IS and BCA. Due to the “routable protocol communications” CIP-005 R1 would be applicable, and there should already be an ESP.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

NST sees no reason to change the existing approved definition's use of "remote access client or other remote access technology." The second part of the proposed definition would, as written, apply to any remote connection using a communications path that included routable to serial conversion, regardless of where that conversion took place (e.g., remote location vs. "local," or "inside the BES asset" location). If this is what the SDT intends, NST recommends updating the CIP-005 Technical Rationale document to make this clear. NST is also concerned that as proposed, the revised definition could be interpreted to apply to any Cyber System, not just BES Cyber Systems and associated in-scope devices.

Likes 1	Central Hudson Gas &amp; Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

Thank you for your comments. While it is true that there is some scoping found within NERC Glossary definitions, is only through careful review of the definitions and Standards that a determination of scope of impact can be identified. The SDT chose to modify definitions within our SAR to remove as much scoping language from the definitions as is possible and beneficial, to enable the definition to cover as many scenarios as possible. The intent is to have scope identified through the combination of definition, applicability, and requirement language. Therefore, the scoping is developed through the same process for each bullet in the IRA definition. The language “remote access client or other remote access technology” used in the current version of the IRA definition was removed for clarity based on industry comments in previous drafts.

Michael Russell – Massachusetts Municipal Wholesale Electric Company – 5 – NPCC

Answer	No
Document Name	

Comment

There seems to be an inconsistency between EACMS definition and the CIP-005 R2 requirements:
1) EACMS definition includes a protocol converter for BCS where no ESP exists.
2) New R2 Applicable Systems requires an Intermediate System
3) New R2.7 requires an ESP between the Intermediate System and the BCS
Is the intent of the SDT to require the protocol converter to be an Intermediate System? In the case where no ESP exists, then R2.7 cannot be met.
Suggest change the Applicable Systems in R2.1 to exclude situations without ERC or change R2.7 requirements to exclude situations where protocol converter is used and there is no ESP

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT believes that the definitions and requirement language is consistent as intended.

1. EACMS definition includes a protocol converter for BCS where no ESP exists. True, and only for “those” that perform electronic access control or electronic access monitoring for the BCS (OR ESP).
2. Applicable Systems columns only define where a requirement is applicable. They do not establish a requirement in themselves. If no Intermediate Systems are in use, then there is no applicability. However, if there is IRA, then there may be an issue with compliance to R2 Part 2.1.
3. R2 Part 2.7 requires the IS to be placed such that “routable protocol communications” to the BCS must go through an ESP. This does not require an ESP unless there are routable protocol communications between the IS and BCA. Due to the “routable protocol communications” CIP-005 R1 would be applicable, and there should already be an ESP.

Jennie Wike – Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer	No
Document Name	

Comment

Tacoma Power is concerned that the exception language in CIP-004 R2 Part 2.3 invalidates the inclusion of the applicable system of “medium impact BCS with IRA”. Tacoma Power recommends deleting the “(except for medium impact BCS without ERC)” from the R2 Part 2.3 requirement language.

Additional editorial comment: “Medium” should not be capitalized in CIP-004 R5 Part 5.1 and R5.2, and R6 Part 6.3.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT has made the clarifying changes to align with the intent.	
Tracy MacNicoll – Utility Services, Inc. – 4	
Answer	No
Document Name	
Comment	
It is unclear if a protocol converter meets the proposed definitions for EACMS and EAP. The lack of clarity makes it difficult to apply the new IRA definition when protocol converters are used. The identification of a EAP on a protocol converter could establish an ESP around a BES Cyber System that does not use a routable protocol. The establishment of an ESP would also cause the non-routable BES Cyber System to meet the definition of ERC, which causes a significate increase in the number of applicable CIP requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT does not see that identification of an EAP on a protocol converter would automatically create an ESP around a BCS that is NOT connected to a network via a routable protocol. The requirement for an ESP is only established by CIP-005 R1 Part 1.1 requirement language, which does not apply to BCS not connected to a network via a routable protocol.	
Israel Perez – Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
This should specifically exclude direct access from a TCA. More detail is needed to understand the scope, for ex: are all serial addresses needed.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments.	
Jodirah Green – ACES Power Marketing – 1,3,4,5,6 – MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	No
Document Name	
Comment	
ACES feels the first sub bullet to the IRA definition is overly wordy and is confusing. ACES sugguests: “To a BCS or a defined Electronic Access Point (EAP).” The CIP standards are not concerened with IRA to any other systems besides Applicable Systems/BCS, so scoping the definition to just what NERC/CIP’s definition is, does not allow any scope creep.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. While it is true that there is some scoping found within NERC Glossary definitions, is only through careful review of the definitions and Standards that a determination of scope of impact can be identified. The SDT chose to modify definitions within our SAR to remove as much scoping language from the definitions as is possible and beneficial, to enable the definition to cover as many scenarios as possible. The intent is to have scope identified through the combination of definition, applicability, and requirement language. Therefore, the scoping is developed through the same process for each bullet in the IRA definition.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	

ISO-NE supports the ISO/RTO Council comments in this area.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments, please see response to the ISO/RTO council.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The standard drafting team has done a good job in clearly defining the scope of IRA.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	

Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern supports the proposed changes for the IRA definition to address IRA in routable to nonroutable (i.e., IP to serial) conversion.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to the IRA definition.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
It appears there may be a discrepancy in the use of BES and BPS. The revised definition of BES Cyber Asset (BCA) includes the following: "Reliable Operatin of the Buld Electric System (BES) while the term Reliable Operation in the Glossary includes: "Operating the element of the Bulk-Power System ..."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT asserts that the use of Reliable Operation covers the essence of how a BCA should be defined and the further wording of "Reliable Operation of the Bulk Electric System (BES)" scopes the definition down to only the elements of the BES. This same wording is also used in the Reliability Co-Ordinator definition	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the modifications to the IRA definition, CIP-005 (Requirement R2) and CIP-004 (Applicable Systems) that address IRA in routable to nonrouteable (i.e., IP to serial) conversion scenarios.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes

Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment, please see response to EEI.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

2. ***The SDT modified other (not related to IRA) definitions used in the CIP standards based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal*.**

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

ACES feels the way the definition of Electronic Access Point (EAP) is written in this draft is overly wordy. ACES suggests:

”An electronic policy enforcement point or a Cyber Asset interface on Electronic Access Control or Monitoring Systems that controls routable communication to and from BES Cyber Systems.”

ACES feels the way the definition of Intermediate System is written in this draft is overly wordy. ACES suggests:

“Electronic Access Control or Monitoring Systems (EACMS) used to restrict Interactive Remote Access to only authorized users”

ACES also noted that the definition of an Intermidiate System no longer states that it must not be located inside an ESP, combined with the removal of the language from R2.1: “such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.” Without those two statements IRA could be initiated through an ESP to an Intermediate System located in an ESP. ACES feels the removal of the language from the definition and requirement is not what was intended and needs to be added back to ensure the security of IRA. Furthermore

with the removal of the language, it allows a Cyber Asset IRA client to connect directly to Applicable Systems, if the Intermediate System is also an EACMS with an EAP. In this scenario the Cyber Asset client connects to the EACMS using a VPN client and Multi Factor Authentication. Once connected to the Intermediate System, the IRA Client could connect directly to applicable systems. There are other scenarios, but this is the most obvious.

EACMS is already plural. so adding “one or more” to the definition of Intermediate System is redundant.

ACES feels the second bullet point on the new Management Interface should be scoped down. There are a variety of vulnerabilities in "autonomous subsystems" in which one could gain access to a system's console. Changing the scope of the definition to be ONLY those devices specifically designed and or used to allow access to a console would reduce scope creep. ACES suggests:

"Is an autonomous subsystem, specifically designed and or used to provide access to the console independently of the Cyber Asset's CPU, firmware, and operating system;"

ACES feels the first word in bullet point one, section 4, of the TCA definition should be "to" rather than "on"

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

The SDT asserts that an EAP may also be controlling routable communication to PCAs and EACMS within the ESP, so limiting the definition to BCS may not be appropriate.

The SDT asserts that the Intermediate System may be made of one EACMS, thus one or more is appropriate.

The SDT asserts that the change to the Intermediate System definition removes requirements out of the definition. Please see CIP-005-8 Requirement R2.7 and the Technical Rationale for changes to definitions.

The SDT asserts that VPN Gateway and IRA tunnel connection from the client to the Applicable System would be logically a direct connection and does not meet CIP-005-8 Requirement R2.7

The SDT asserts that limiting the second bullet of the Management Interface definition to lights out console type access only would not cover interfaces that allow for remote power control

The SDT asserts that one or more EACMS is needed to cover the case of a single system

The SDT asserts that in the TCA definition, ”on” a network better describes the intent of the definition	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
Glossary, changes cause us to read many glossary terms to understand the term, then go to read standard and see how changes to glossary term has impact to the standard. EX: Management Interface. Definition should include physical interface or process, not both within the same definition. EX: term ‘unauthorized’ used, focus on the risk of unauthorized change. How is unauthorized defined?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments The SDT asserts that it was tasked to clean up definitions by removing requirements and make them broader. Scoping has been moved to either the Applicable Systems column or within the requirement language itself. The SDT asserts that the Management Interface definition should describe it in a broad sense and that the scoping is done within the Applicable Systems column (SCI supporting an Applicable System ...) and the requirement language (Protect ESP and SCI configuration…) The SDT asserts that definitions/meanings of terms like “authorized”/“unauthorized”, “vendor”, etc. should be explicitly defined by the entity within their own compliance programs	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	

Answer	No
Document Name	
Comment	
PCA Definition – routable protocol missing. Please clarify ESP criteria / demarcation considerations if a Reponsible Entity takes a “policy” or ruleset based approach to an ESP; in relation to PCAs. Examples involving firewall / VLans / Switch controls… Can a Responsible Entity Choose what devices are PCAs based on the policy? The first bullet is missing the concept of being explicitly connected by a routable protocol Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.... Suggest …. Are connected to a network using a routable protocol and are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments The SDT asserts that within the PCA definition of “being protected by an ESP” already implies that routable protocol is being used The SDT understands that there are complex issues around documenting ESP policy, especially in a hybrid networking situation. The SDT will be proposing that Implementation Guidance on ESP policy be created by one of the prequalified organizations.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	

Comment
NST respectfully offers the following comments on proposed new and revised definitions: Intermediate System: NST recommends maintaining the "not within an ESP" language from the current definition rather than having that component be implied by a requirement part. Management Interface: NST recommends changing, "An administrative interface,..." to, "A dedicated physical or logical administrative interface,..." Electronic Security Perimeter: NST believes the proposed new part of the current ESP definition, “or a logical boundary defined by one or more EAPs” is redundant and unnecessary. We therefore recommend maintaining the currently approved ESP definition. Virtual Cyber Asset: NST suggests including some of the wording found in the definition of "Cyber Asset," such as, "including software and data." NST notes that the proposed definition, as written, would make it possible for a VCA to be hosted on a BES Cyber Asset that is itself a VCA. If this is what the SDT intends, NST recommends modifying the definition to make this clear. Electronic Access Control and Monitoring System: NST sees no need for modifying the existing definition. We also note that not all protocol converters perform access control and/or monitoring, which makes it inappropriate to include them in a revised definition of EACMS. External Routable Connectivity: As we did in 2022, NST believes the use of the word, "through (an ESP)" has the potential to cause confusion over the kind(s) of routable communications that may qualify as ERC. ERC to or from a Cyber Asset should be clearly defined as "through" an ESP boundary or access point, not "through" an ESP. The online Merriam Webster dictionary defines "through" as "a function word to indicate movement into at one side or point and out at another and especially the opposite side of // 'drove a nail through the board'". NST believes the existing definition of ERC can and should be retained as-is. Shared Cyber Infrastructure: NST recommends adding "hardware" to "One or more programmable electronic devices, including the software,..." NST also recommends adding language to either or both of the "Cyber Asset" and "SCI" definitions that clarifies a device that hosts and/or provides storage resources for BES Cyber Systems and associated virtual devices at a single impact level (e.g., high) should be identified as a Cyber Asset, not as SCI.

Electronic Access Point: As we did in 2022, NST believes the proposed definition of EAP is problematic in two respects. First, we believe it could be interpreted to mean an EAP should control all routable communication between a BCS and any other Cyber Asset regardless of whether that "other" device is within or outside of the same ESP protecting the BCS. Second, we believe the SDT should better define "policy enforcement point" lest Responsible Entities, Regional Entities, and NERC develop their own conflicting definitions.

Transient Cyber Asset: As we did in 2022, NST notes the proposed definition includes a statement ("Virtual machines hosted on a physical Transient Cyber Asset (TCA) are treated as software on that physical TCA.") that directly conflicts with a statement included in the proposed definition of Cyber Asset ("VCAs are not considered software or data of Cyber Assets.").

Likes 1	Central Hudson Gas &amp; Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

Thank you for your comments

The SDT asserts that it was tasked with removing requirements from its definitions, therefore it is appropriate that the Intermediate System definition does not contain its location relative to an ESP. This has been moved to CIP-005 Requirement 2.7

The SDT asserts that the Management Interface definition also needs to cover both non-dedicated physical and non-dedicated logical interfaces which may be used to manage ESP or SCI configuration such as those running on SCI management systems

The SDT asserts that the ESP definition requires “boundary” for forward compatibility in zero trust model and “border” for backwards compatibility.

The SDT asserts that for the definition of VCA, where “SCI and Cyber Assets that host VCAs” are excluded is appropriate as is. Adding an additional description to the Cyber Assets wording such as “SCI and Cyber Assets including software or data, that host VCAs” may cause additional confusion as to which asset is these are associated with. The SDT asserts that the situation of VCAs running on a VCA is already addressed as intended.

The SDT asserts that the ERC definition required changes to cover zero trust models which do not have the concept of inside or outside of an ESP

The SDT asserts that the SCI definition reference to "devices" already covers hardware. The SDT will be proposing that Implementation Guidance on all-in vs SCI be created by one of the prequalified organizations. The SDT recognizes that ESP policy and how this relates to EAP and ESP policy enforcement can be a complex area, especially in hybrid situations. The SDT will be proposing that Implementation Guidance on ESP policy be created by one of the prequalified organizations. The SDT asserts that the EACMS definition requires changes to address protocol converter that are used to provide IP connectivity to BCS The SDT asserts that the TCA definition is as intended and that it is appropriate that virtual machines, running on a TCA , as not being VCAs	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments. PCA Definition – routable protocol missing. Please clarify ESP criteria / demarcation considerations if a Reponsible Entity takes a "policy" or ruleset based approach to an ESP; in relation to PCAs. Examples involving firewall / VLans / Switch controls… Can a Responsible Entity Choose what devices are PCAs based on the policy? The first bullet is missing the concept of being explicitly connected by a routable protocol Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.... Suggest…. Are connected to a network using a routable protocol and are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments. Please refer to the response for NPCC	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	
PCA Definition – routable protocol missing. Please clarify ESP criteria / demarcation considerations if a Reponsible Entity takes a “policy” or ruleset based approach to an ESP; in relation to PCAs. Examples involving firewall / VLans / Switch controls… Can a Responsible Entity Choose what devices are PCAs based on the policy? The first bullet is missing the concept of being explicitly connected by a routable protocol *Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or....* Suggest …. Are connected to a network using a routable protocol *and are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or.*	
Likes 0	
Dislikes 0	
Response	
The SDT asserts that within the PCA definition of “being protected by an ESP” already implies that routable protocol is being used	

The SDT understands that there are complex issues around documenting ESP policy, especially in a hybrid networking situation. The SDT will be proposing that Implementation Guidance on ESP policy be created by one of the prequalified organizations.

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer	No
Document Name	

Comment

LCRA believes the current CIP-002 SAR regarding serial-IP converters should be resolved prior to defining them as an EACMS.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.
The SDT asserts that this is part of the SAR for Project 2021-03 CIP-002

Teresa Krabe - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

LCRA believes the current CIP-002 SAR regarding serial-IP converters should be resolved prior to defining them as an EACMS.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.
The SDT asserts that this is part of the SAR for Project 2021-03 CIP-002

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

The suggested definitions are mixing the concepts and they are making the overall understanding complicated. For example, the identification of PCA’s is done through CIP-005. CIP-002 defines the BES that defines the BCS, and at the end the BCA. It’s not written in CIP-002 that BCA need to be defined.

No where in the standard is the PCA is directly defined. The first time you see it is in part 1.1 of the R1 table in CIP-005.

For example, we have a BCA and we have a Cyber Asset they are communicating using a routable protocol, they are in the same network. Both Cyber Assets have an IP address. Theses Cyber Assets are connected via a routable protocol, thus they are in a ESP and the non qualified Cyber Asset is the PCA. In this case, the PCA is protected by an ESP.

Going with a different example, we have a BCA and we have a Cyber Asset they are communicating using a non routable protocol, there’s no network and both Cyber Asset don’t have an IP address. Those Cyber Asset are not connected via a routable protocol; thus they are not in an ESP and the non qualified Cyber Asset is nothing.

The second bullet of the PCA definition is a bit complicated, there’s the mention of “isolates routable connectivity”. We are no longer into PERMIT or DENY we are isolating, but we are still linked by the routable connectivity, ie routable protocol.

The part that is getting more confusing is the definition of the ESP. The definition of ESP has two concepts, one is based on routable protocol which works with 1.1 of CIP-005, the other is based on a logical boundary defined by one or more Electronic Access Points (EAP). What is a logical boundary ? Is a logical boundary based on routable protocol? To add to the confusion the EAP is a policy enforcement interface and it’s related to an EACMS. Is a policy a ruled based on routable protocol? Which requirement is asking to document this policy? Is it CIP-005R1.2? How to we evaluate the policy ?

Regarding the EACMS definition, which is again build with two concepts. One of the concept is “, including those not protected by an Electronic Security Perimeter used by the responsible entity to convert routable protocol communications to non routable communications to a BCS”. Considering how the current proposed standard is written, a converter (routable protocol communications to non routable communications) is associated to IRA. And IRA is associated to the concept of Intermediate System, and Intermediate System is tag as an EACMS. This logic is establish with the current proposed standard. What is the added value to add this concept to the definition of EACMS ? Overall it seems that the SDT tried to answer multiple objectives (concepts) with the same term/definition. The end result is that we have variations in the definition and the terms are cascading. The SDT should make the definition simpler and limit the number of cascades (ESP->EAP->EACMS) . Definitions are there to ease the understanding or support the requirements, they shouldn’t add additional controls.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the response for NPCC The SDT asserts that additional CIP-002 criteria and requirements for the identification of PCAs, EACMS and SCI is part of the SAR for Project 2021-03 CIP-002 The SDT understands that there are complex issues around ESP policy, EAP and EACMS, especially in a hybrid networking situation. The SDT will be proposing that Implementation Guidance on ESP policy be created by one of the prequalified organizations. The SDT asserts that a protocol converter allowing IP connectivity to a BCS is performing the EACMS function, therefore it is appropriate to add this to the EACMS definition.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	

AEPC has signed on to ACES comments:

ACES feels the way the definition of Electronic Access Point (EAP) is written in this draft is overly wordy. ACES suggests:

”An electronic policy enforcement point or a Cyber Asset interface on Electronic Access Control or Monitoring Systems that controls routable communication to and from BES Cyber Systems.”

ACES feels the way the definition of Intermediate System is written in this draft is overly wordy. ACES suggests:

“Electronic Access Control or Monitoring Systems (EACMS) used to restrict Interactive Remote Access to only authorized users”

ACES also noted that the definition of an Intermidiate System no longer states that it must not be located inside an ESP, combined with the removal of the language from R2.1: “such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.” Without those two statements IRA could be initiated through an ESP to an Intermediate System located in an ESP. ACES feels the removal of the language from the definition and requirement is not what was intended and needs to be added back to ensure the security of IRA. Furthermore

with the removal of the language, it allows a Cyber Asset IRA client to connect directly to Applicable Systems, if the Intermediate System is also an EACMS with an EAP. In this scenario the Cyber Asset client connects to the EACMS using a VPN client and Multi Factor Authentication. Once connected to the Intermediate System, the IRA Client could connect directly to applicable systems. There are other scenarios, but this is the most obvious.

EACMS is already plural. so adding “one or more” to the definition of Intermediate System is redundant.

ACES feels the second bullet point on the new Management Interface should be scoped down. There are a variety of vulnerabilities in “autonomous subsystems” in which one could gain access to a system’s console. Changing the scope of the definition to be ONLY those devices specifically designed and or used to allow access to a console would reduce scope creep. ACES suggests:

“Is an autonomous subsystem, specifically designed and or used to provide access to the console independently of the Cyber Asset’s CPU, firmware, and operating system;”

Likes 0	

Dislikes 0	
Response	
Thank you for your comments. Please refer to the ACES response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	

HQ supports NPCC RSC comments and provides the following additional comments:

The suggested definitions are mixing the concepts and they are making the overall understanding complicated. For example, the identification of PCA's is done through CIP-005. CIP-002 defines the BES that defines the BCS, and at the end the BCA. It's not written in CIP-002 that BCA need to be defined.

No where in the standard is the PCA is directly defined. The first time you see it is in part 1.1 of the R1 table in CIP-005.

For example, we have a BCA and we have a Cyber Asset they are communicating using a routable protocol, they are in the same network. Both Cyber Assets have an IP address. Theses Cyber Assets are connected via a routable protocol, thus they are in a ESP and the non qualified Cyber Asset is the PCA. In this case, the PCA is protected by an ESP.

Going with a different example, we have a BCA and we have a Cyber Asset they are communicating using a non routable protocol, there's no network and both Cyber Asset don't have an IP address. Those Cyber Asset are not connected via a routable protocol; thus they are not in an ESP and the non qualified Cyber Asset is nothing.

The second bullet of the PCA definition is a bit complicated, there's the mention of "isolates routable connectivity". We are no longer into PERMIT or DENY we are isolating, but we are still linked by the routable connectivity, ie routable protocol.

The part that is getting more confusing is the definition of the ESP. The definition of ESP has two concepts, one is based on routable protocol which works with 1.1 of CIP-005, the other is based on a logical boundary defined by one or more Electronic Access Points (EAP). What is a logical boundary ? Is a logical boundary based on routable protocol? To add to the confusion the EAP is a policy enforcement interface and it’s related to an EACMS. Is a policy a ruled based on routable protocol? Which requirement is asking to document this policy? Is it CIP-005R1.2? How to we evaluate the policy ?

Regarding the EACMS definition, which is again build with two concepts. One of the concept is “, including those not protected by an Electronic Security Perimeter used by the responsible entity to convert routable protocol communications to non routable communications to a BCS”. Considering how the current proposed standard is written, a converter (routable protocol communications to non routable communications) is associated to IRA. And IRA is associated to the concept of Intermediate System,
and Intermediate System is tag as an EACMS. This logic is establish with the current proposed standard. What is the added value to add this concept to the definition of EACMS ?

Overall it seems that the SDT tried to answer multiple objectives (concepts) with the same term/definition. The end result is that we have variations in the definition and the terms are cascading. The SDT should make the definition simpler and limit the number of cascades (ESP->EAP->EACMS) . Definitions are there to ease the understanding or support the requirements, they shouldn’t add additional controls.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Please refer to the HQ5 response

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	

Comment

NCPA recommends the following edits:

Cyber System should say "Two or more Cyber Assets...." as the word system implies multiples devices working together.

The proposed Intermediate System definition removed the requirement of not being inside the ESP, however in the proposed language for CIP-005-8 R2.7 it states "...communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP", which implies that it must reside outside of the ESP. NCPA suggests keeping the original language in the Intermediate System to include not being located within an ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT asserts that a Cyber System can consist of 1 Cyber Asset , therefore this is appropriate The SDT asserts that it was tasked with removing requirements out of the Intermediate System definition. The requirement language was moved from the definition to CIP-005 R2.7	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
SCI is superfluous considering that existing classification definitions can be applied. SCI does not clearly state what devices would be included and which are not included. Cyber Systems definition seems to rope in non-CIP assets. BES Cyber Systems definition is sufficient for grouping together Cyber Assets.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments.

The SDT asserts that SCI definition is as intended and that the Applicable Systems column in the requirements performs the scoping required to narrow down the applicability. The SDT will be proposing that Implementation Guidance on the aspects of All-in vs SCI be created by one of the prequalified organizations.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by ACES.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please refer to the ACES response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
The definition of Intermediate System remains ambiguous as to whether it can cover such devices as Active Directory servers or firewalls. The terminology should be changed to define the Intermediate System to be the device that IRA is restricted to, not the device that does the restriction (which is not the Intermediate System, but is the firewall and/or domain policy server).	

Also, the definition of BES Cyber Asset (BCA) uses the Glossary Term "Reliable Operations". This definition of BCA could increase the scope of the Cyber Assets being used for the operation of the BES since Reliable Operations defines Bulk-Power System's method of operation (which is a broader less precise term than BES). Lastly the use of the term "Management Interface" needs clarification with use case and pertinent examples.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT asserts that the Intermediate System definition is as intended. The entity must evaluate all systems needed for the function of the Intermediate System and classify them appropriately. The SDT asserts that the use of Reliable Operation covers the essence of how a BCA should be defined and the further wording of “Reliable Operation of the Bulk Electric System (BES)” scopes the definition down to only the elements of the BES. This same wording is also used in the Reliability Co-Ordinator definition The SDT will be proposing that Implementation Guidance on Management Interfaces be created by one of the prequalified organizations.	
Micah Runner - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	
Black Hills Corporation has the following comments regarding the CIP definition changes:	

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like: "Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. (Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.)" **EAP:** The definition should be revised to include the following commas to ensure clarity of the definition: "An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets."	
Likes 0	
Dislikes 0	
Response	
Thank you for your response The SDT discussed your proposed changes to the Cyber Asset definition. The current positioning and phrasing are needed for the definition to work as intended. The SDT discussed your proposed changes to the EAP definition. The current positioning and phrasing are needed for backwards compatibility	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	No
Document Name	
Comment	
Black Hills Corporation has the following comments regarding the CIP definition changes:	

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like: "Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. (Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.)" **EAP:** The definition should be revised to include the following commas to ensure clarity of the definition: "An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets."	
Likes 0	
Dislikes 0	
Response	
Thank you for your response The SDT discussed your proposed changes to the Cyber Asset definition. The current positioning and phrasing are needed for the definition to work as intended. The SDT discussed your proposed changes to the EAP definition. The current positioning and phrasing are needed for backwards compatibility	
Josh Combs - Black Hills Corporation - 3	
Answer	No
Document Name	
Comment	
Black Hills Corporation has the following comments regarding the CIP definition changes:	

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like: “Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. (Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.)” **EAP:** The definition should be revised to include the following commas to ensure clarity of the definition: “An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your response The SDT discussed your proposed changes to the Cyber Asset definition. The current positioning and phrasing are needed for the definition to work as intended. The SDT discussed your proposed changes to the EAP definition. The current positioning and phrasing are needed for backwards compatibility	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	No
Document Name	
Comment	
Black Hills Corporation has the following comments regarding the CIP definition changes:	

Cyber Assets: The last two sentences of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like: “Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. (Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.)” **EAP:** The definition should be revised to include the following commas to ensure clarity of the definition: “An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.”

Likes 0	
Dislikes 0	

Response
Thank you for your response The SDT discussed your proposed changes to the Cyber Asset definition. The current positioning and phrasing are needed for the definition to work as intended. The SDT discussed your proposed changes to the EAP definition. The current positioning and phrasing are needed for backwards compatibility

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	

The BCA definition changes include the defined term "Reliable Operation" which applies to the BPS by definition rather than just the BES. AECI supports the use of the previous "reliabile operation" undefined term as it would eliminate the risk of scope expansion to non-BES assets.

Likes 0	
Dislikes 0	

Response

Thank you for your response . The SDT asserts that the use of Reliable Operation covers the essence of how a BCA should be defined and the further wording of “Reliable Operation of the Bulk Electric System (BES)” scopes the definition down to only the elements of the BES. This same wording is also used in the Reliability Co-Ordinator definition

Lindsey Mannion - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The new Electronic Security Perimeter (ESP) definition still complicates the situation with respect to mixed-trust environments where a Responsible entity may choose to create ESPs and corresponding EAP’s per individual Cyber System (zero trust paradigm). While this may be easier with standalone physical Cyber Assets – introducing SCI, VCA, virtual clusters, and virtual networking creates complexity that could allow unauthorized access if not carefully configured for applicable VM guests and virtual networks – especially if affinity controls are not strictly created and enforced. Marrying both ESP and zero-trust within an overall ESP would better serve our Responsible Entities and create a more secure environment as zero-trust Cyber Assets would not be directly internet-facing. Maintaining the ESP, and fully incorporating virtualization and zero trust paradigms within an identified ESP allows Responsible Entities to leverage another layer of defense (defense-in-depth) for Applicable Systems by limiting ingress/egress points and access to these BCS.

For the Shared Cyber Infrastructure definition, where is this to be identified and categorized? CIP-002 only requires the identification of BCS while the associated Technical Rationale warns of Assets with Multiple Classifications regarding high water marking. Is the entity to assume SCI must be included in CIP-002 even though it is not specifically included in the BCS definition?

Likes 0	
Dislikes 0	

Response

Thank you for your comments

The SDT will be proposing that Implementation Guidance on ESP policy / Zero Trust be created by one of the prequalified organizations

The SDT asserts identification of SCI (as well as EACMS and PCAs) is now within the scope of Project 2021-03 CIP-002

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC have the following comments regarding the CIP definition changes:

Cyber Assets: The last two sentence of the definition should be included as a note to the definition so that the term Cyber Asset is not in the definition of a Cyber Asset. Here is an example of what that could look like:

“Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices.

(Note – Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.)”

Cyber System: The definition should be changed to the following: “Two or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure working together to provide or perform a specific function.”

EAP: The definition should be revised to include the following commas to ensure clarity of the definition: "An electronic policy enforcement point, or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems, that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets."

BCA: The proposed BES Cyber Asset (BCA) definition now capitalizes "Reliable Operation", which describes/ defines how to operate the **Bulk Electric System (BES)**. However, Reliable Operations specifically refers to the **Bulk-Power System** in its definition:

"Operating the elements of the ***[Bulk-Power System]*** *within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."*

The Bulk-Power System is defined as:

"(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

(B) electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. (Note that the terms "Bulk-Power System" or "Bulk Power System" shall have the same meaning.)"

The Bulk-Power System term is broader in scope and less precise than the Bulk Electric System term. The Bulk Electric System is defined as:

"...all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy..."

With the capitalization of "Reliable Operations", it could be interpreted that the proposed definition of BCA could increase the scope of the Cyber Assets used for operating the BES since Reliable Operations describes/defines how to operate the Bulk-Power System, which is a broader less precise term than BES.

SMUD and BANC would like to understand why the defined term, Reliable Operation, was used and if the intent of the revision is to broaden the scope of Cyber Assets.

Likes 0	

Dislikes 0	

Response

Thank you for your comments
Cyber System, Cyber Asset, EAP

The SDT asserts that the Cyber Asset definition was carefully crafted to work as intended and that the proposed change may have unintended consequences.

The SDT asserts that the Cyber System definition is as intended and meant to be inclusive / shorthand so as to be used in situations where separately specifying Cyber Assets, VCAs and SCI repeatedly would have been excessively wordy and caused confusion

The SDT asserts that the EAP definition was crafted as-is for backward compatibility purposes .

The SDT asserts that the use of Reliable Operation covers the essence of how a BCA should be defined and the further wording of “Reliable Operation of the Bulk Electric System (BES)” scopes the definition down to only the elements of the BES. This same wording is also used in the Reliability Co-Ordinator definition

Tracy MacNicoll - Utility Services, Inc. - 4

Answer	Yes
Document Name	

Comment

USV support the comments made by NPCC RSC.

The proposed ESP definition uses the terms “border” and “boundary”. It is unclear what difference is between these two terms and how this difference impacts the proposed definition.

Likes 0	
Dislikes 0	

Response	
Thank you for your comments . Please refer to the NPCC response The SDT asserts that “boundary” is forward compatible with zero trust networking and “border” is required for backwards compatibility. Please refer to the CIP-005-8 Technical Rationale	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
In the CIP Senior Manager definition, the words "cyber security" should be deleted. As proposed it implies that the CSM is no longer responsible for physical security Standards CIP-006 & CIP-014.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments The SDT asserts that the title of the CIP-006 Standard includes the words “Cyber Security” The SDT asserts that CIP Senior Manager is not associated with CIP-014 and also that “Cyber Security” is not in the title for CIP-014	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	

AZPS supports the changes to definitions within draft 5.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the changes made to the definitions as posted in this Draft 5 posting.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the definition changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees and supports the changes to the definitions in Draft 5.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	

Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The work the standard drafting team has done to move requirements out of the definitions and in to the standards improves the reliability standards overall.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	

Answer	Yes
Document Name	
Comment	
ISO-NE supports the ISO/RTO Council comments in this area.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA has two recommendations: Cyber Asset definition: recommend improving the grammar by rewriting so there is not an “excluding” phrase separated from an “including” phrase by nothing but a comma. As written it will cause confusion. ERC definition: Given that the EAP definition would be modified to refer to EACMS as the ‘location’ of the EAP, the definition of ERC might read better if it stated “through an EAP” or “through its EACMS” rather than "through its ESP.”	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments.

The SDT asserts that the Cyber Asset definition was carefully crafted as-is and that changes may have unintended consequences
The SDT asserts that the ERC definition was crafted to be both forward compatible with zero trust networking as well as backwards compatible

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

FirstEnergy does not opposed the other definitions.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

3. ***The SDT revised CIP-005 R1 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.***

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC disagree with the new definitions for IRA and Cyber System as the proposed definition changes may expand the scope of CIP-005, Requirement R1 to non-BES Cyber Systems.

Likes 1	Central Hudson Gas &amp; Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

The SDT asserts that the purpose of the IRA glossary term is to describe a certain type of access, without scoping the security requirements on such access within the term’s definition. The actual scope of and required controls on IRA are contained within CIP-005 R2. It is in R2 where the generic “Cyber System” in the definition of IRA is appropriately scoped. The SDT asserts the NERC glossary should function solely as a dictionary and all mandatory requirements and scoping of such requirements should be in the standards themselves. Positively, this avoids situations where an entity is essentially “non-compliant” with a requirement or scope included in a glossary definition, therefore they are potentially non-compliant with all requirements in the standard that rely on that definition.

The SDT notes that CIP-005 R1 does not refer to IRA and does not agree, nor is it the intent, that the IRA definition expands the ESP scope to non-BCS, with the exception of the PCAs within the ESP.

Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
As with Draft 4, BPA does not support the expansion of R1, Part 1.6 to include the protection of data traversing communications links. Expansion to communications links does not consider devices that cannot meet this criterion. Putting communication links in scope would increase costs and maintenance activities and would require re-architecture of links. BPA does support the replacement of “protect” with “permit” in R 1 Part 1.3; this adds clarity to the intent of the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for the support of the changes to R1.3. As to Requirement Part 1.6, the SDT notes this new Requirement Part is a combination of scenarios where a single ESP is extended between different PSPs and thus access to this network is not physically protected while between PSPs. To date, this has been the purview of CIP-006 R1.10, however that was designed for “across the hall” LAN scenarios and it was limited to cabling and non-programmable components (i.e., unmanaged hubs/switches, patch panels, etc.). For virtualization purposes, the SDT needed to incorporate true WAN scenarios with flat networks (thus a single ESP) so that VCAs could seamlessly move from hypervisors in one physical data center to another physical data center over large distances, increasing reliability and resiliency of those VCAs’ functions. The SDT chose to simplify this by incorporating CIP-006 R1.10 scenarios (“across the hall”) with this larger “Super-ESP”scenario (“across the state”) so that there is one single requirement in one standard that addresses all scenarios where a single ESP must exit one PSP and extend to another. Along with this multi-site WAN scenario, the existing exemption 4.2.3.2 in the CIP standards would not exclude any Cyber Assets between the sites, such as the carrier’s equipment because it is not “between discrete ESPs”; it is all within the same ESP and thus all that equipment would be, at minimum, PCAs within the ESP. That is an unintended consequence of the desire to extend a flat ESP across sites	

to increase resiliency of VCAs moving seamlessly between sites. The SDT therefore added a new exemption 4.2.3.3 that will exclude Cyber Assets to address this while working hand-in-hand with this new Requirement Part 1.6. The end result is the responsible entity is required to protect the data while it is between PSPs and can do so either in the previous CIP-006 R1.10 way for short distances or in the new R1.6 way for long distances and then may exempt the Cyber Assets between the encryption points where the data is protected. The SDT asserts this consolidates all the scenarios, removing the local one from CIP-006 R1.10 and combining it all into this new R1.6 in CIP-005 whose scope is protecting the ESP.

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

The STD proposed a change to specify EAP as applicable systems. BC Hydro recommends providing additional clarity on evidence expectations where network-like evidence is expected at the BCS level.

Likes 0	
Dislikes 0	

Response

The SDT notes that EAP is not used in the Applicable Systems column for R1 and its Parts. It is used in the example measures for R1.2 as “EAP configuration”. Previous drafts did include EAP as an applicable system but that is no longer the case.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
Document Name	

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF) and ACES.

Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to MRO NSRF and ACES.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
NCPA does not agree based on comments made in question 1 related to the proposed IRA definition change.	
Likes 0	
Dislikes 0	
Response	
Thank you, please see response to Q1 in regards to IRA definition change.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
HQ supports NPCC RSC comments and provides the following additional comments: R1.2 We support the following modification “excluding time sensitive communications of Protection Systems” (replacing “communications using protocol IEC TR 61850-90-5 R-GOOSE”) assuming that the intentof the SDT was to link with the definition of Protection System (Glossary of terms)	

In the column Measures, the SDT mentions VLAN and VXLAN, they are not routable protocoles. Please refer to the OSI model.

R1.3 The objective of Requirement R1.2 is to protect the BCA and the PCA through the management of the routable protocol communications (Permit/Deny). The EACMS and SCI assist in the delivery of the BCA/PCA functionalities. The EACMS and SCI Management interface are just as important, we suggest wording the requirement R1.2 and R1.3 the same way. R1.2 could be worded as: “Protect Applicable System by implementing policy enforcement to permit only needed network accessibility documenting the reason, and deny all other communications, through the ESP.” Doing so would removed the need of R1.3 or would be more “inline”.

Please note the usage of the word policy, this usage is to ensure a logical link between the requirements and the definitions.

The definition of ESP brings the concept of routable protocol and the concept of logical boundary.

R1.4 This requirement should consider including the introduction of Management interface concept. Management interface is another mean to interact with the Cyber Asset and should be address.

Likes 0	
Dislikes 0	

Response

Thank you for your support of R1.2 and the SDT agrees the intent is to link to the “Protection System” in the NERC Glossary of Terms.

In the Measures for R1.2, the SDT does use examples of VLAN and VXLAN *configuration* and agrees that while those are not OSI layer routable protocols in and of themselves, their configuration could be used as methods to “Permit only needed routable protocol *communications*”.

For R1.3, the SDT thanks you for the suggestion but asserts that two separate Requirement Parts are necessary. R1.2 is scoped to the Applicable Systems protected by (inside) the ESP while R1.3 is to protect the Management Interface of the Cyber Assets creating and controlling the ESP (thus not protected by the ESP itself). Should R1.2 and R1.3 be combined, the SDT foresees a “hall of mirrors” possibility. Also, the SDT believes R1.2 should NOT include a “per system capability” option but R1.3 should due to varying capability of Management Interfaces, thus necessitating separate Requirement Parts. The SDT also notes that while these are separate Parts, it is one single Requirement R1.

For R1.4, the SDT did not consider Dial-Up Connectivity changes as part of our SAR. Around the ESP definition, the SDT retained the existing language and added new language for zero trust
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	
Comment	

AEPC has signed on to ACES comments:

ACES feels R1.3 should be reworded:

“EACMS, and their supporting SCI, that control access to and from an ESP for an Applicable System in Part 1.1”

ACES feels in R1.4: “if any” is not necessary.

Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to ACES.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	No
Document Name	
Comment	

HQ supports NPCC RSC comments and provides the following additional comments:

R1.2 We support the following modification “excluding time sensitive communications of Protection Systems” (replacing “communications using protocol IEC TR 61850-90-5 R-GOOSE”) assuming that the intentof the SDT was to link with the definition of Protection System (Glossary of terms)

In the column Measures, the SDT mentions VLAN and VXLAN, they are not routable protocoles. Please refer to the OSI model.

R1.3 The objective of Requirement R1.2 is to protect the BCA and the PCA through the management of the routable protocol communications (Permit/Deny). The EACMS and SCI assist in the delivery of the BCA/PCA functionalities. The EACMS and SCI Management interface are just as important, we suggest wording the requirement R1.2 and R1.3 the same way. R1.2 could be worded as: “Protect Applicable System by implementing policy enforcement to permit only needed network accessibility documenting the reason, and deny all other communications, through the ESP.” Doing so would removed the need of R1.3 or would be more “inline”.

Please note the usage of the word policy, this usage is to ensure a logical link between the requirements and the definitions.

The definition of ESP brings the concept of routable protocol and the concept of logical boundary.

R1.4 This requirement should consider including the introduction of Management interface concept. Management interface is another mean to interact with the Cyber Asset and should be address.

Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to Hydro-Quebec comments (Nicolas Turcotte) above.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	

1.3 broaden from *network accessibility* to be more objective = *"protect configuration"* in order to allow other methods to protect the configuration *Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability*. Suggest *Implement methods to protect ESP and SCI configurations at Management Interfaces of Applicable Systems, per system capability, per system capability.*	
Likes 0	
Dislikes 0	
Response	
Thank you for the suggestion. The intent of adding "Protect the ESP and SCI configurations" was to add the objective, the "why", behind the required action of permitting only needed network accessibility to the Management Interface. In the proposed language, the SDT considers implementing these methods "at" the Management Interface may be too prescriptive and could remove some needed flexibility. For example, the intent may be met by implementing a dedicated management zone in the infrastructure to which the Management Interface is connected. In this instance, the method is not implemented "at" the Management Interface in question, however the objective can be met from methods implemented elsewhere.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments. 1.3 broaden from network accessibility to be more objective = "protect configuration" in order to allow other methods to protect the configuration	

Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability. Suggest Implement methods to protect ESP and SCI configurations at Management Interfaces of Applicable Systems, per system capability, per system capability.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see response to NPCC RSC comments above.	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Part 1.5 -> Suggestion to consider IPS/IDS on the edge of a facility instead of between discrete ESPs (E.g. if a facility has a number of ESP and non-ESP network segments, but has IPS/IDS controls at the routing edge of the facility) Part 2.6 -> Use wording from CIP-007 that explicitly excludes storage resources (consistency in language) Part 2.7 -> It could be clearer if this requirement just explicitly states that the intermediate system is required to be outside of the ESP that it is providing access to. The requirement to route through an EAP is then covered by R1.2 and not needed to re-stated in this requirement.	
Likes 0	
Dislikes 0	
Response	

In regards to Part 1.5, the SDT is not changing the intent, only making necessary conforming changes to allow for perimeter-less technology such as some Zero Trust installations. The SDT notes that in the currently approved CIP-005-7, Part 1.5 does imply the detection must be at the EAP as that is the Applicable System. To the point raised, the Applicable System is now the BCS and it no longer prescribes nor implies where on the network the method must be implemented, only that the method can be shown to detect the communications entering or leaving the ESP and thus may be upstream. The SDT believes the currently proposed R1.5 better incorporates the suggested scenario and allows the entity to take the encouraged step of detecting malicious communications in an even broader scope than what is strictly required by the CIP standard.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	No
Document Name	

Comment

As we did in 2022, NST objects to the use of the phrase "through the ESP," as in, "Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP;..." (R1.2). Data packets don't go "through" an ESP, they go into or out of an ESP through an access point.

NST also notes that while R1.3 requires a Responsible Entity to control network access to the Management Interfaces of SCI, there is no comparable requirement for devices (e.g., Hypervisors) that are not SCI according to the SDT's proposed definition but that still host virtual machines that are in scope for R1. This inconsistency should be addressed.

Likes 1	Central Hudson Gas &amp; Electric Corp., 1, Ridolfino Michael
Dislikes 0	

Response

Thank you for the comment. The intent of “through the ESP” is to better incorporate future Zero Trust implementations where there is no “logical border surrounding a network” but instead Policy Enforcement Points at the accessed resource itself or as close to it as possible. In these instances that are designed to be perimeter-less, the concepts of “inside” and “outside” begin to fail and the SDT is removing those now to be better prepared for future technologies. The SDT asserts that even in traditional Layer 3 firewalls that define an ESP, the communications between systems that are encapsulated in packets go “through” the perimeter (ESP) in order to reach their destination.

As to the scoping of R1.3 to SCI, the SDT notes that for hypervisors that are not SCI because they are considered BCS or PCA, the hypervisors will be categorized the same as the VCAs they host and thus R1 will apply as well as CIP-007 R1 to the hypervisor itself. The SDT asserts the concern is addressed by these other requirements. R1.3 is bringing in two scenarios that would not otherwise be addressed.

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC

Answer	No
Document Name	

Comment

1.3 broaden from network accessibility to be more objective = “protect configuration” in order to allow other methods to protect the configuration

Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.

Suggest

Implement methods to protect ESP and SCI configurations at Management Interfaces of Applicable Systems, per system capability, per system capability.

Likes 0	
Dislikes 0	

Response

Thank you. Please see the response to NPCC RSC above.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

Thank you for your comment. No, due to lack of understanding of scope of impact to our systems. Better understanding of ‘applicable systems’ is needed. Provide examples. Implementation plan guidance needed to better understand how to be in compliance.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT would be glad to respond to specific examples of unclear scope. Section 4.3 of the standards (above the requirement section) is where the term “Applicable Systems” is defined within the standards. While the SDT has not produced Implementation Guidance (which usually documents a single way to implement), it has produced much material in the Technical Rationale documents related to these changes that the SDT hopes will be helpful.

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	

Comment

ACES feels R1.3 should be reworded:

“EACMS, and their supporting SCI, that control access to and from an ESP for an Applicable System in Part 1.1”

ACES feels in R1.4: “if any” is not necessary.

Likes 0	
Dislikes 0	

Response

Thank you for your proposed change. The SDT has carefully crafted the current applicability based on comments from previous drafts and asserts the suggested language would broaden it beyond the intended scope. An example will help regarding this one specific piece of the Applicable Systems column. The SDT is focused on Management Interfaces that define/create or are “on” the ESP and thus control it. It is not the intent to include all EACMS that are outside the ESP (but could be included in the proposed phrasing of “control access to and from an ESP”). For example, the intent is to include the Management Interface of a network switch that is configured with a VLAN that is part of the ESP and another VLAN that is not. Thus, the switch “controls” the ESP by defining what is and is not the ESP. The management port on a firewall is similar, controlling what is and is not the ESP. Then consider a domain controller outside the ESP that is an EACMS and part of an Intermediate System – it has no “Management Interface” of the sort where you can control its network accessibility such as putting an ACL on a port as one example. It does help enforce access authentication and authorization for access to the ESP, but it doesn’t control the ESP itself. This distinction is why the SDT has used the language it has chosen.

Regarding Part 1.4 and the “if any”. The SDT agrees it is not strictly necessary, but as the SDT was making conforming changes to handle the “per system capability” language, the intent was to help lessen the burden on entities as dial-up becomes obsolete. Since the overall Requirement includes “shall implement one or more documented processes that…”, adding “if any” may help those entities that no longer have any dial-ups and thus do not need to implement a documented process for a non-existent technology in their environment.

Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment	
FirstEnergy does not opposed these changes.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
ISO-NE supports the ISO/RTO Council comments in this area.	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see responses to the ISO/RTO Council comments.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The standard drafting team has done an excellent job in addressing comments in CIP-005 and compliance to the new wording is backwards compatible. Manitoba Hydro notes that the definition of Intermediate System was updated to remove the phrase “The	

Intermediate System must not be located inside the Electronic Security Perimeter" and requirement R2.7 was added requiring "Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.". The new requirement does not make it clear that an EACMS that contains an EAP cannot also be the intermediate system. The following wording is suggested to clarify that a separate system such as a "jump host" must be used as an Intermediate System:

"Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an EAP in a separate Cyber Asset or Virtual Cyber Asset."

Likes 0	
Dislikes 0	

Response

Thank you for your encouraging words regarding our work on CIP-005.

On the issue raised regarding R2.7, the SDT does not intend to prescribe architecture to the point of what CA or VCA a function may reside. For example, some "security appliances" that have firewall/EAP capability also have separate functionality within them that can perform part of the Intermediate System function. Historically this definition has stated "must not be located inside" which allowed for "outside or ON" the ESP. The SDT does not want to preclude architectures where at least some portion of the Intermediate System functionality may execute on the EAP.

Mark Flanary - Midwest Reliability Organization - 10

Answer	Yes
Document Name	

Comment

While we can agree with the changes as they stand, should circumstances arise where additional changes to CIP-005 are necessary, we offer the following recommendations:

Part 1.3 - We recommend against the changing of "to and from" to simply "to". Controlling outbound communication is vital protection to prevent connectivity of a compromised system out to a comand-and-control server.

Part 2.3 - Consider the scenario of low impact SCI as the initiating system. The requirement phrase "Cyber Asset or Virtual Cyber Asset" excludes SCI from the set of possible initiating systems. We recommend updating the language to encapsulate all forms by using the defined term "Cyber Systems" or adding SCI.

Likes 0	
Dislikes 0	

Response

Thank you for the recommendations.

For Part 1.3, the SDT concluded that when speaking specifically of Management Interfaces on SCI and EACMS, while there are several ways to control the traffic to such interfaces, many such interfaces may not have the capability for outbound filtering. The intent is to block access to the ‘front door’ of the ability to configure/reconfigure these particular types of systems. In some situations, such as the SCI hosting a BCS within an ESP, the Management Interface will also inherit numerous CIP required controls, in addition to this Requirement Part which would be in addition.

Richard Vendetti - NextEra Energy - 5

Answer	Yes
Document Name	

Comment

NEE supports EEI comments

Likes 0	
Dislikes 0	

Response

Thank you. See response to EEI comments.

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	
Comment	
Southern agrees and supports the changes to the Applicable Systems, Requirements, and Measures in CIP-005 R1.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to CIP-005 Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	

The standard drafting team has done an excellent job in addressing comments in CIP-005. The NSRF notes that the definition of Intermediate System was updated to remove the phrase “The Intermediate System must not be located inside the Electronic Security Perimeter” and requirement R2.7 was added requiring “Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.”. The new requirement does not make it clear that an EACMS that contains an EAP cannot also be the intermediate system. The following wording is suggested: “Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an EAP in a separate Cyber Asset or Virtual Cyber Asset.”	
Likes 0	
Dislikes 0	
Response	
Thank you. Please see the response to the similar comment from Manitoba Hydro above.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you. See response to EEI comments.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes

Document Name	
Comment	
EEI supports the changes made to CIP-005, Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you. See response to EEI comments.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	

Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you. See response to EEI comments.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Thank you.	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
USV supports the comments made by NPCC RSC	

The R1.5 requirement language limits the scope of this requirement to "routable communication entering or leaving an ESP". Suggest moving this scoping language to the applicability column by adding "with ERC" to both high and medium impact BCS listed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT notes that for R1.5 if the scoping phrasing was removed and moved into a "with ERC" phrase in the Applicable Systems column, which would scope to systems with a certain kind of connectivity, but would leave it unclear exactly what traffic requires the malicious communication detection. It could inadvertently broaden the scope from the traffic entering or leaving the ESP (north/south) to all east/west traffic on all networks within the ESP which is not the intended scope.	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

4. The SDT revised CIP-007 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments submitted by the ISO/RTO Council (IRC) Standards Review Committee (SRC) and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please refer to the IRC response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes R1.3 needs to be re-worded to make it clear it applies to SCI hosting both high and medium impact BES Cyber Systems if a Responsible Entity doesn't want "high water marking" to compel treating the medium impact BCS as PCAs associated with the high impact BCS.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. The SDT will be proposing that Implementation Guidance on affinity be created by one of the prequalified organizations	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	No
Document Name	
Comment	
Part R1.3 -> The requirement outlines controls/evidence recommended for non-BCS VCAs sharing SCI, but does not provide options potential options of classifying/securing non-BCS VCAs where physical/logical isolation cannot be achieved or is finacially restrictive.	
Likes 0	
Dislikes 0	
Response	
Thank You for your response The SDT will be proposing that Implementation Guidance on affinity be created by one of the prequalified organizations	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	No
Document Name	
Comment	
HQ supports NPCC RSC comments and provides the following additional comments:	

R1.1 The requirement "Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. " This requirement is ambiguous and the column measure is still referencing logical ports. Furthermore, how will this requirement will be evaluated ? The previous version of this requirement was less ambiguous.

R1.3 the definition of SCI includes the storage resource but this requirement exclude the storage resources. How is the shared storage resources managed ? What about the shared network resource ?

For some requirements the TFE was removed for "per system capability."We do understand that TFE process isn't optimal but it permitted more nuance than per system capability. For example, the TFE basis for approval of a technical feasibility exception are, at least the two following points;

{C}(i) is not technically possible or is precluded by technical limitations; or

{C}(ii) is operationally infeasible or could adversely affect reliability of the Bulk Electric System to an extent that outweighs the reliability benefits of Strict Compliance with the Applicable Requirement;

Per system capability is only equal to the first point but doesn't equal to the second or to the other three. The SDT should define per system capability.

Likes 0	
Dislikes 0	

Response

Thank you for your response

The SDT asserts that multiple controls are available (overlay, underlay, zero trust) to meet the network accessibility requirement and the entity needs to demonstrate which controls are used. The SDT will be proposing that Implementation Guidance on network accessibility be created by one of the prequalified organizations

The SDT asserts that the Management Interface definition and SCI definition make it clear that management systems associated with storage resources are in scope and that the storage resource itself is excluded (i.e., virtual disk/LUN). The SDT will be proposing that Implementation Guidance on affinity be created by one of the prequalified organizations

The SDT suggests contacting NERC Compliance as to how to document “system capability” for those requirements were “per Cyber Asset capability” was previously used

Nicolas Turcotte - Hydro-Quebec (HQ) - 1

Answer	No
Document Name	

Comment

HQ supports NPCC RSC comments and provides the following additional comments:

R1.1 The requirement “Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability. “ This requirement is ambiguous and the column measure is still referencing logical ports. Furthermore, how will this requirement will be evaluated ? The previous version of this requirement was less ambiguous.

R1.3 the definition of SCI includes the storage resource but this requirement exclude the storage resources. How is the shared storage resources managed ? What about the shared network resource ?

For some requirements the TFE was removed for “per system capability.”We do understand that TFE process isn’t optimal but it permitted more nuance than per system capability. For example, the TFE basis for approval of a technical feasibility exception are, at least the two following points;

(i) is not technically possible or is precluded by technical limitations; or

(ii) is operationally infeasible or could adversely affect reliability of the Bulk Electric System to an extent that outweighs the reliability benefits of Strict Compliance with the Applicable Requirement;

Per system capability is only equal to the first point but doesn’t equal to the second or to the other three. The SDT should define per system capability.

Likes 0	
Dislikes 0	

Response	
Thank you for your response. Please refer to the HQ5 response above	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	
SCI is superfluous considering that existing classification definitions can be applied. SCI does not clearly state what devices would be included and which are not included. Cyber Systems definition seems to rope in non-CIP assets. BES Cyber Systems definition is sufficient for grouping together Cyber Assets.	
Likes 0	
Dislikes 0	
Response	
Thank You for your response The SDT will be proposing that Implementation Guidance on All-in vs SCI be created by one of the prequalified organizations	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	
The ISO/RTO Council (IRC) Standards Review Committee (SRC) requests clarification of the term “network accessibility” used within requirement R1 Part1.1, which reads as follows: “Disable or prevent unneeded routable protocol **network accessibility** on each Applicable System, per system capability.” One of the measures also references this term: “Identity or process based access policy or workload configuration demonstrating needed **network accessibility**.” Specifically, the SRC requests that the drafting team clarify whether entities will need to define the term “network accessibility” in their documented processes or whether a standardized definition	

will apply. If there is a specific definition that entities are intended to use, the SRC requests that the SDT provide the definition that will apply.

Likes 0	
Dislikes 0	

Response

Thank you for your response. The SDT asserts that multiple controls are available (overlay, underlay, zero trust) to meet the network accessibility requirement and the entity needs to demonstrate which controls are used.

The SDT will be proposing that Implementation Guidance on network accessibility be created by one of the prequalified organizations

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	No
Document Name	

Comment

SMUD and BANC appreciate the Standard Drafting Team’s work to modify CIP-007. However, we note that the word “system” is used inconsistently, especially with regards to “per system capability”, and this makes the High and Medium impact requirements less stringent than the requirements for Low impact. We recommend changing the language to “per Cyber Asset capability.”

Likes 0	
Dislikes 0	

Response

Thank you for your response

The SDT suggests contacting NERC Compliance as to how to document “per system capability” for those requirements were “per Cyber Asset capability” was previously used.	
James Keele - Entergy - 1,3,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren would like clarity on the change from where technically feasible to per system capability. Does this mean that the TFE process is going away or are they changing it to a different name?	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT suggests contacting NERC Compliance as to how to document “per system capability”	

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Thank you for your response	

Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response	

Daniel Gacek - Exelon - 1	
Answer	Yes

Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the changes made to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	

ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to CIP-007.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees and supports the changes made to CIP-007.	

Likes 0	
Dislikes 0	
Response	
Thank you for your response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
BC Hydro agrees with the changes however seeks further clarification as follows. BC Hydro seeks clarification with use cases or examples on proposed changes to CIP-007 R1.1, whether, “per system capability” means entities are compelled to install software (if possible) that can be used to block network accessibility? Specifically, if a Cyber Asset uses a	

method (e.g.: host firewall) that can block the unneeded network accessibility, but that method has been determined to be detrimental to reliable operations, does this mean entities are compelled to continue to use that method although it affects the operation? BC Hydro also seeks clarification on Routable protocol network accessibility particularly, as Technical Feasibility Exception (TFE) is replaced by "per system capability", are the entities expected to make decisions on whether to document or not to document exceptions on per system capability? Please provide some use case examples and further guidance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT asserts that multiple controls are available (overlay, underlay, zero trust) to meet the network accessibility requirement and the entity needs to demonstrate which controls are used. The SDT will be proposing that Implementation Guidance on network accessibility be created by one of the prequalified organizations The SDT suggests contacting NERC Compliance as to how to document “per system capability” for those requirements were “per Cyber Asset capability” was previously used	
Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.	
Likes 0	

Dislikes 0	
Response	
Thank you for your response The SDT discussed your proposed change. The SDT asserts that the wording was intentional as “within” does not support zero trust networking. The SDT will be proposing that Implementation Guidance on affinity be created by one of the prequalified organizations	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response for Black Hills Corp	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	

Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response for Black Hills Corp	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with the comments from Public Utility District No. 1 of Chelan County: in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see the response for Black Hills Corp	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
BPA notes that implementation of and documenting compliance with Part 1.1 may pose technical challenges depending on an entity’s architecture or processes.	
Likes 0	
Dislikes 0	
Response	
The SDT asserts that multiple controls are available (overlay, underlay, zero trust) to meet the network accessibility requirement and the entity needs to demonstrate which controls are used. The SDT will be proposing that Implementation Guidance on network accessibility be created by one of the prequalified organizations	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Consider rewording R1.3 for clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response The SDT reviewed the wording for R1.3 . The SDT concluded that it was intentional . The SDT will be proposing that Implementation Guidance on affinity be created by one of the prequalified organizations	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	Yes
Document Name	
Comment	
FirstEnergy does not opposed these changes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response	
Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
CHPD agrees with the proposed changed to CIP-007 R1.3. We would also like to express our support for the decision to remove the Electronic Access Control and Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) from the list of applicable systems in CIP-007 R1.3. This change is a positive step forward, as it helps support backward compatibility with the standard. However, in our review of the proposed changes, we identified an opportunity to enhance the clarity of the requirement section of R1.3. Our proposed wording for R1.3 is as follows: Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are within an ESP, and VCAs that are not within an ESP.	

We believe this reworded requirement maintains the original intent of the section while making it more straightforward and easier to understand. By replacing "VCAs that are, or are associated with, a medium or high impact BCS" with "VCAs that are within an ESP," we simplify the language while preserving the core security objectives of the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response. The SDT discussed your proposed change. The SDT asserts that the wording was intentional as “within” does not support zero trust networking. The SDT will be proposing that Implementation Guidance on affinity be created by one of the prequalified organizations	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ben Hammer - Western Area Power Administration - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes

<table>
<tr><td>Document Name</td><td></td></tr>
<tr><td colspan="2">Comment</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Likes 0</td><td></td></tr>
<tr><td>Dislikes 0</td><td></td></tr>
<tr><td colspan="2">Response</td></tr>
<tr><td colspan="2">Thank you for your support.</td></tr>
<tr><td colspan="2">John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway</td></tr>
<tr><td>Answer</td><td>Yes</td></tr>
<tr><td>Document Name</td><td></td></tr>
<tr><td colspan="2">Comment</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Likes 0</td><td></td></tr>
<tr><td>Dislikes 0</td><td></td></tr>
<tr><td colspan="2">Response</td></tr>
<tr><td colspan="2">Thank you for your support.</td></tr>
<tr><td colspan="2">Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI</td></tr>
<tr><td>Answer</td><td>Yes</td></tr>
<tr><td>Document Name</td><td></td></tr>
<tr><td colspan="2">Comment</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Likes 0</td><td></td></tr>
<tr><td>Dislikes 0</td><td></td></tr>
</table>

Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

5. ***The SDT made numerous clarifying changes to CIP-010 based on industry comments. Do you agree with the proposed changes? If not, please provide the basis for your disagreement and an alternate proposal.***

James Keele - Entergy - 1,3,6

Answer	No
Document Name	

Comment

Entergy disagrees with CIP-010 R1.1 as written for two reasons.

First, the requirements as written is difficult to follow as a single sentence with many oxford commas and could benefit from a rewrite to reduce confusion. Entergy proposes the requirement be rewritten similar to the following:
"Authorize changes that affect Applicable Systems and alter the behavior of one or more cyber security controls (as defined by the Responsible Entity) that serve one or more requirement parts in CIP-005 or CIP-007. This excludes procedural and physical controls."
Secondly, Entergy is concerned regarding the removal of the previous CIP-010 R1.4 language that allowed an assessment of potentially impacted security controls, the ambiguity of the "as defined by the Responsible Entity" language, and how this could expand the scope of testing and change authorization.
As written the standard implies that any potential change to a control "defined by the Responsible Entity" would require authorization and subsequent testing, which would result in Responsible Entity security controls testing expanding from a list of potentially impacted security controls to a verification of all security controls regardless on the actual nature of the change to prove a control wasn't impacted.
As written the "defined by the Responsible Entity" could be interpreted as being related to the defining of the controls, not the defining by the Responsible Entity of a change to a control.
Entergy believes the intent of this requirement is still to perform authorizations and testing of potential and identified impacts to CIP-005 and CIP-007 controls prior to deployment. This is supported by the proposed CIP-010 R1.4 language to "verify the behavior(s) of the altered cyber security controls" which implies a verification of a pre-determined set of impacts, not a verification of ***all*** controls.
If Entergy is interpreting this correctly, then Entergy proposes that CIP-010 R1.1 be rewritten to something similar to the following, which replaces "defined" with "determined":

“Authorize changes that the Reponsible Entity determines will affect Applicable Systems and alter the behavior of one or more cyber security controls that serve one or more requirement parts in CIP-005 or CIP-007. This excludes procedural and physical controls.”

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT recognizes the complexities of the requirement language, and appreciates the concern. The SDT was mindful of comma placement and conforms with the NERC style guide. The SDT intent is consistent with the security objectives as articulated in your comments, as a primary goal was to maintain backwards compatibility while adding the appropriate level of flexibility to enable for virtualization. The SDT considered the suggestion to replace “defined” with “determined” in Requirement Part 1.1 and determined “defined” was the appropriate term because it is referring to the controls in scope for the change authorization process. Using the word “determined” could be interpreted as more subjective and could create the need for potentially exhaustive evidence to justify to an auditor for each change how the entity determined the authorization was required in each instance, whereas “defined” becomes a documented finite set of cyber security controls the entity expects change authorization for because of the way the cyber security control(s) serve one or more requirement parts in CIP-005 or CIP-007 for that entity . As a result, the SDT has not made this modification.

Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	No
Document Name	

Comment

The problem with the current standard verbiage is that there is no requirement for a baseline, but there is no way to accomplish what the standard requires without creating baselines to monitor. Knowing you are going to be making a change that affects the baseline is a much more straightforward measure than trying to predict which/if any changes will affect CIP-005 or CIP-007 security controls tests and to what extent these should be re-tested after a change that may or may not affect the test results. For example in R1.2 the measure to include evidence such as "…a list of differences between the production and test environments with descriptions of how any differences were accounted for" cannot be accomplished without a baseline to compare against.

R2.1's requirement is unclear whether we should be monitoring for different test results, or if we should be monitoring for changes to a baseline (again, there is no mention of baselines so I'm not convinced this is a valid interpretation). If it is the case that we need to test all CIP-005 and CIP-007 controls (except physical and procedural), these are the bulk of bookending tasks for any new system. Performing this for hundreds of devices monthly is not feasible. We are a smaller entity, and we can't imagine how a larger entity could perform hundreds or thousands of bookends every month. In Attachment 2 Section 2.1 there are two instances of the same typo for "..Responsible Entity **that that** document.."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT considered your comments and suggestions that Requirement R2 monitoring cannot be accomplished without Requirement R1 'baselines'. The SDT maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement with 'baselines' as one means to achieve the objective. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. The terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. maintains backwards compatibility and clarity that an entity may choose to continue to use baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", for which those changes then require authorization per Requirement R1 Part 1.1. Requirement R2 Part 2.1 monitoring applies to a subset of the changes authorization per Requirement R1 Part 1.1.as a function of its applicability to high impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA, and SCI supporting an Applicable System in Requirement R2 Part 2.1. SDT's scoping of methods to monitor for "...unauthorized changes that alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement part CIP-007, as defined by the Responsible Entity." further assures this requirement is not misinterpreted as a mini audit of CIP-005 and CIP-007, but is that subset of CIP-007-related changes authorized per Requirement R1 Part 1.1. The mapping of Measures by mapping to the former 'baseline' attributes further demonstrates 'baselines' remain one way how an entity may choose to demonstrate compliance. The SDT determined the scoping and applicability was clear and appropriate and did not make modifications to Requirement R2 Part 2.1. Thank you for calling out the typos, the SDT has addressed them.	

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	

SMUD and BANC do not agree with the changes to CIP-010 for the following reasons:

- CIP-010 should be reverted to its current state with the simple addition to the “Applicable Systems column” with the newly added SCI, like how it is being done for the CIP-007 revisions, to accommodate for the addition of SCI.

- The Technical Feasibility Exception was removed and not replaced with “per system capability?” If an entity has an approved TFE for CIP-010-4 R1.5, the changes proposed in CIP-010-5 R1.2 would now be applicable to that entity with no relief. Therefore, with CIP-010-5 R1.2 the entity would now be noncompliant.

- The Technical Rational for Requirement R2 is “to keep the scope of R2 to those things for which there are an ***automated solution*** that can monitor these areas and alert entities to changes.” Additionally, “The SDT also added “***per system capability***” in recognition that not all changes in scope can be monitored on every potential in-scope Cyber System. This addition makes the requirement conditional if a system is incapable of monitoring a particular unauthorized change category.” However, there is no mention that CIP-010-5 R2 Part 2.1 is only applicable for automated solutions and no automated solutions are excluded. Is that assumed/implied/allowed with the “***per system capability***” statement? Furthermore, in the Measures it states, “Examples of evidence may include, but are not limited to, reports generated from ***automated tools or manual reviews*** along with records of investigation for any unauthorized changes that were detected.” This statement causes further confusion for which the Standard Drafting Team (SDT) should address.

- The SDT should clarify if the term “per system capability” applies to Parts 2.1.1 through 2.1.7. The language that precedes the Parts reads, “...that include ***at least one cyber security control for each of the following***:” which refutes the “per system capability” statement. Is there a way for the SDT to incorporate the “per system capability” for each sub-requirement?

Likes 0	

Dislikes 0	

Response

Thank you for your comments. The SDT appreciates the perspective shared about reverting to former approved, but maintains the shift from prescriptive requirements to objective level requirements is necessary to enable the standards for virtualization, as well as to permit new and emerging technologies, features and tools moving into the future. For this reason, the SDT did not revert nor modify the proposed requirement language.

The SDT contends the proposed changes to Requirement R1 negate the need for both the “technically feasible” and “per system capability” because the focus is on testing the implemented CIP-005 and/or CIP-007 cybersecurity controls the responsible entity determines as serving the requirements in CIP-005 and CIP-007 and require authorization. If a particular CIP-005 or CIP-007 cyber security control cannot be implemented due to technical infeasibility or per system capability, then that unimplemented cyber security control would not be in scope for CIP-010-5 Requirement R1, nor former Requirement Part 1.5 (which is Part 1.2 in the final draft). Please see the Technical Rationale (TR) for more information.

The SDT reviewed the requirement language and measures for CIP-010-5 Requirement R2 Part 2.1 and does not intend for the ‘per system capability’ language to exclude manual monitoring methods from the scope of Part 2.1. The SDT’s intent when using the ‘per system capability’ language is to keep the scope of R2 to those things for which automated solutions are available and likely to monitor these areas and alert entities to changes. It should be noted that the ‘system’ in ‘per system capability’ refers to the Applicable Systems for the requirement, and not the capability of the automated tool used to monitor. As a result, the ‘per system capability’ language does not absolve entities of the obligation to implement monitoring methods where automated solutions have not been implemented, and while potentially less ideal, manual methods to accomplish the same results where automated monitoring cannot be done remains a requirement where the Applicable System is capable of producing data related to the list of seven cyber security-related categories to monitor. TR has been updated to include this clarification.

The TR has been updated to recognize that the automated monitoring output (alarms, alerts, reports, logs etc.) may require manual review by the recipients to determine if the detected change was unauthorized and what subsequent actions, if any, may need to be taken, and to provide clarity on the intention of the reference to manual reviews as records in the measures.

The SDT intends for the ‘per system capability’ language in Requirement Part 2.1 to be transitive and applicable to all of the listed subparts 2.1.1 – 2.1.7 and maintains that where one of those seven security controls is not relevant to the implementation of the entity’s

Applicable Systems, it renders the obligation moot. If an entity has not implemented VCA on SCI within their Applicable Systems, the entity would not be subject to Part 2.1.2 because there is nothing to monitor. The TR was reviewed, and includes statements reflecting the SDT also added “per system capability” in recognition that not all changes in scope can be monitored on every potential in-scope Cyber System. This addition makes the requirement conditional if a system is incapable of monitoring a particular unauthorized change category.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
R1-Removing baseline configuration does not change what needs to be done in practice. Entities will still need to retain a baseline configuration as evidence from which to establish the changes that were authorized. For Part 1.1 an entity will still need to show the baseline configuration prior to the change to show required cyber security controls in CIP-005 and CIP-007 are not adversely affected. For Part 2.1 an entity will still need to provide baseline configurations for evidence that they monitor at least once every 35 calendar days for unauthorized changes to the items listed Parts 1.1 and 1.2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT maintains that establishing and maintaining a baseline is one way an entity may comply with CIP-010-5, and for entities that choose that method, the SDT agrees the revised Standard is backwards compatible and the Measure and accompanying evidence would be consistent with that which an entity might use today to demonstrate compliance. Where an entity chooses other methods, the evidence for Part 2.1 would not require baselines configurations themselves. The Measures provide options for how an entity could demonstrate the automates monitoring methods used for the cyber security controls the entity	

defined in Requirement R1 as serving the requirements in CIP-007, in combination with the output of those monitoring methods, and supporting investigation documentation of detected unauthorized changes.	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	No
Document Name	
Comment	

ISO-NE supports the ISO/RTO Council comments in this area, which are replicated here:

ISO/RTO Council is looking for clarification regarding the R2 requirement language that is mandating specific and prescriptive security controls to be monitored for change relevant to CIP-007 standard. In particular, the proposed requirement language of "… that include at least one cyber security control for each of the following…" is the area of confusion. See underlined section within the proposed requirement language below:

"Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following:

2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility;

2.1.2. Configuration of CPU or memory sharing of VCAs on SCI;

2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.

2.1.4. Configuration of malicious code protection methods;

2.1.5. Configuration of security event logging or alerting;

2.1.6. Configuration of authentication methods; and

2.1.7. Changes to the enabled or disabled status of accounts.” ISO/RTO Council would like for the SDT to clarify if the intent of this requirement is to monitor for changes to all of the CIP-007 controls? If this is meant to be defined by the entity, ISO-NE recommends moving the sub-bullets language to the measures section similar to R1. ISO-NE adds the following comment: With respect to the proposed 2.1.7 sub-requirement, changes to account access should be considered part of CIP-004 Access Management as a subject and not be administered from the CIP-007 requirements. ISO-NE recommends striking the 2.1.7 sub-requirement if the sub-requirements are retained in the proposed version of CIP-010 R2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please also refer to the SDT response for ISO/RTO Council.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
With respect to R1.4, BC Hydro seeks clarity, if evidence from a representative test system is sufficient OR if evidence from a production system(s) is also required in all cases. Requirement R1.4 uses "behavior" which is a very open term and can be used in many ways. BC Hydro seeks clarity on this with examples or use cases to explain the scope of the word behavior.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The Applicable Systems is the subject of the requirement and examples of evidence can be found in the Measures. The SDT has developed Technical Rationale, which describes the reasoning behind the terminology used in CIP-010. The SDT will be deferring to the pre-qualified organizations for the industry development of Implementation Guidance to help assure there is an owning group that can maintain it over time.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer	No
Document Name	

Comment

The SRC requests clarification regarding the language in requirement R2 that mandates the use of specific and prescriptive security controls to be monitored for changes relevant to the CIP-007 standard. In particular, the SRC requests clarification of the proposed requirement language of "… that include at least one cyber security control for each of the following…." See the underlined section within the proposed requirement language below:

"Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; **that include at least one cyber security control for each of the following**:

2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility;

2.1.2. Configuration of CPU or memory sharing of VCAs on SCI;

2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.

2.1.4. Configuration of malicious code protection methods;

2.1.5. Configuration of security event logging or alerting;

2.1.6. Configuration of authentication methods; and

2.1.7. Changes to the enabled or disabled status of accounts." The requirements contained in the draft of CIP-007-7 have a combined total of 21 Parts, but the draft CIP-010-5 R2 language only lists seven controls (Parts 2.1.1 – 2.1.7). It is therefore unclear whether R2 is intended to require entities to monitor for changes that impact all CIP-007 controls or only for changes that impact the items listed in R2. The SRC requests that the SDT clarify this ambiguity. If the intent is for entities to determine which controls to include in their monitoring to detect changes that would impact CIP-007 protections, the SRC recommends moving the language in Parts 2.1.1 – 2.1.7 to the measures section, similar to the way the measures section associated with requirement R1 Part 1.1 is structured.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT has used the phrasing "that include at least one cyber security control for each of the following" in order to allow entities to monitor a primary security control if they have multiple overlapping controls. The SDT's intent is that having multiple security controls over these categories is a good and beneficial practice where possible, and entities should not be discouraged from having more than one. This phrasing's intent is to allow the entity to choose the primary control they monitor for unauthorized change. The entity may of course do more than one, but one is required. Additionally, the SDT also added "per system capability" in recognition that not all changes in scope can be monitored on every potential in-scope Cyber System. This addition makes the requirement conditional if a system is incapable of monitoring a particular unauthorized change category. The SDT performed and extensive analysis of the CIP-007 requirement parts, as compared to the former baseline attribute model and concluded the seven parts are a minimum set of cyber security controls (technical controls) that must be implemented and monitored for unauthorized changes to the Applicable Systems in Part 2.1. The language does not preclude entities from choosing to go above and beyond the minimums of the standard based on their risk tolerance. Please see the TR for additional information on the intent of each of the seven components.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	No
Document Name	
Comment	

NIPSCO disagrees with the changes as “security controls” needs to be better scoped and defined.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. CIP-010-5 scopes “security controls” by assuring the consistent use of the phrase ‘cyber security controls’, and through reference to those which serve the requirement parts of CIP-005 and CIP-007. The focus of CIP-005 and CIP-007 and their requirement parts is to implement technical controls that protect the cyber security posture of the logical environment and the systems that comprise or support it. The focus of CIP-010-5 is authorizing changes that affect the security posture of those Applicable Systems, and monitoring for unauthorized changes to the technical controls that have been implemented to maintain that cyber security posture. The Measures provide examples of potential evidence, and the TR provides details on the SDT’s intent as it relates to the scope of the applicable ‘cyber security controls’ that serve CIP-005 and CIP-007.	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
Answer	No
Document Name	
Comment	
There appears to be inconsistency in the CIP-010-5 proposed draft language for Requirements R1 (authorization) and R2 (monitoring). The draft R2 language is more prescriptive for a set of CIP-007 controls while the draft R1 language is now non-prescriptive and related to the “behavior” of CIP-005 and CIP-007 controls, which is subjective and does not align with the list of CIP-007 controls listed in the draft R2 language. In addition, the CIP-010-5 proposed draft language is unclear whether R2 is intended to require entities to monitor for changes that impact all CIP-007 controls or only for changes that impact the items listed in R2. SPP recommends keeping the currently approved requirement language of CIP-010-4, Requirements R1 and R2, as entities have already established virtualized environments that comply with CIP-010-4 today.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments. The scoping of Requirement R2 is an intentional subset of the scope for Requirement R1. The focus of CIP-010-5 Requirement R1 is authorizing changes that affect the security posture of those Applicable Systems as well as the logical environments that protect them. This is why R1 includes the obligation to authorize changes that alter the behavior of one or more cyber security controls that are implemented to protect the system or environment. The Applicable Systems for the R2 monitoring requirement for unauthorized changes is an intentional a subset of cyber security controls (CIP-007) to align with the Appliable Systems scope and those technical controls that have been implemented at the System or Cyber Asset level to maintain that cyber security posture. In Requirement R2 Part 2.1 the SDT's intention is to scope the monitoring to the seven listed items, per system capability. Additionally, the SDT also added "per system capability" in recognition that not all changes in scope can be monitored on every potential in-scope Cyber System. This addition makes the requirement conditional if a system is incapable of monitoring a particular unauthorized change category. The SDT has used the phrasing "that include at least one cyber security control for each of the following" in order to allow entities to monitor a primary security control if they have multiple overlapping controls. The SDT's intent is that having multiple security controls over these categories is a good and beneficial practice where possible, and entities should not be discouraged from having more than one. This phrasing's intent is to allow the entity to choose the primary control they monitor for unauthorized change. The entity may of course do more than one, but one is required. The SDT performed and extensive analysis of the CIP-007 requirement parts, as compared to the former baseline attribute model and concluded the seven parts are a minimum set of cyber security controls (technical controls) that must be implemented and monitored for unauthorized changes to the Applicable Systems in Part 2.1. The language does not preclude entities from choosing to go above and beyond the minimums of the standard based on their risk tolerance. Please see the TR for additional information on the intent of each of the seven components. The SDT appreciates the perspective shared about reverting to former approved, but maintains the shift from prescriptive requirements to objective level requirements is necessary to enable the standards for virtualization, as well as to permit new and emerging technologies, features and tools moving into the future. For this reason, the SDT did not revert nor modify the proposed requirement language.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	

The proposed language removes the baseline requirements that had previously outlined specifically what needed authorization change requests and has been replaced with referencing all of CIP-005 and CIP-007 controls. As the standards evolve over time this makes is unclear and left open for interpretation of what changes an Entity must consider for authorization requests for compliance purposes vs. “best practices”. NCPA recommends including language in 1.1 to include the specific criteria that an Entity will be held accountable to in the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT considered your comments about the removal of 'baselines' from Requirement R1 and maintains the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement with 'baselines' as one means to achieve the objective. The SDT determined the focus of the requirements should remain at an objective level of 'what' is required, instead of getting into 'how'. The terminology, "as defined by the Responsible Entity." within Requirement R1 Part 1.1. maintains backwards compatibility and clarity that an entity may choose to continue to use baselines as the method to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", for which those changes then require authorization per Requirement R1 Part 1.1. Ultimately it is up to each Registered Entity to define their process in a manner that ensures those changes serving one or more requirement parts in CIP-005 or CIP-007 are authorization per Requirement R1 Part 1.1, and that evidence exists to demonstrate those authorizations.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
HQ supports NPCC RSC comments and provides the following additional comments: Considering the ambiguity of the controls defined in CIP-005 5 and CIP-007 the updated version of Table R1, part 1.1 deteriorates the cyber security of the cyber assets,. The Measures column contains more explicit examples than the requirement themselves. As an	

example, for CIP-007 the requirement is “Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.”. The column Measures of CIP-007 R1.1 contains the following : • Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) The SDT should ensure that controls are clearly defined in CIP-005 and CIP-007 .The SDT should also ensure that the requirements are easy measurable, and limit interpretations. The suggested version of requirement 1.3 is defining the applicability by listing the following components; the operating systems, firmware, software, or software patches In the previous version of this requirement, the applicability was 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; and 1.1.5. Any security patches applied. The SDT should evaluate if the intent, of the new version, was it to increase the scope of the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the response to NPCC RSC comments. The SDT maintains the shift from prescriptive requirements to objective level requirements is necessary to enable the standards for virtualization, as well as to permit new and emerging technologies, features and tools moving into the future. Because this approach was built with backwards compatibility in mind, entities may continue to implement a baseline as their process for changes that must be authorized. The SDT maintains the adjustments to Requirement R1 Part 1.3 do not increase scope, but rather reframe the existing obligation without the use of the term baseline. This supports enabling the standard for virtualization. For this reason, the SDT did not revert nor modify the proposed requirement language.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Regarding CIP-010 R1, Texas RE continues to be concerned security obligations will be reduced by removing the reference to baseline configurations. Establishing and maintaining baseline configurations represent best practices for system hardening. Texas RE recommends adhering to NIST Special Publication 800-53 (Rev. 5), CM-2 Baseline Configuration, which states, “Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.” See also CM-7 Least Functionality, which states: Review and update the list of authorized software programs.

Regarding CIP-010 R2, Texas RE is concerned the proposed changes to CIP-010 R1 do not include a control to verify that unintended changes have not been made. For medium impact BCS this is currently captured in requirements to authorize changes and update baseline configuration documentation within 30 calendar days. Texas RE recommends adding medium impact BCS and their associated EACMS and PCA to the Applicable Systems column of CIP-010 R2 and its subpart(s). In FERC Order 706, paragraph 398 FERC states 'We agree with ISO/RTO Council that the phrase “verification that unintended changes have not been made” captures the core issue. Our concern is that some form of verification is performed to detect when unauthorized changes have been made and to identify those changes, as well as ensuring that the proper alerts are issued.'

Further, Texas RE recommends dividing CIP-010 R2 Part 2.1 into two parts for clarity:

CIP-010 R2 Part 2.1:

The Responsible Entity shall define its cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, to include at least one cyber security control from each of the following:

2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility;

2.1.2. Configuration of CPU or memory sharing of VCAs on SCI;

2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.

2.1.4. Configuration of malicious code protection methods;

2.1.5. Configuration of security event logging or alerting;

2.1.6. Configuration of authentication methods; and

2.1.7. Changes to the enabled or disabled status of accounts.

CIP-010 R2 Part 2.2:

The Responsible Entity shall implement methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls defined in Part 2.1.

Likes 0	
Dislikes 0	

Response

Thank you for your comments.

The SDT maintains the shift from prescriptive requirements to objective level requirements is necessary to enable the standards for virtualization, as well as to permit new and emerging technologies, features and tools moving into the future. Because this approach was built with backwards compatibility in mind, entities may continue to implement a baseline as their process for changes that must be authorized

It is outside the scope of the 2016-02 SAR and the virtualization objectives of the SAR to expand the scope of Requirement R2 to include medium impact BCS and their associated EACMS and PCA. For this reason, the SDT maintained the scope proposed in draft 5.

The SDT considered the proposed language to split Part 2.1 into two subparts and appreciates the thought TRE has given to this approach. The SDT agrees it has potential to add clarity and the split would not substantially modify the intent of the proposed language in draft 5. The SDT discussed the unintended consequences of making this potentially clarifying change in the final balloting phase at the risk of it being perceived as substantive, and elected not to make the modification. Again, thank you for this idea.

Junji Yamaguchi - Hydro-Quebec (HQ) - 5

Answer	No
Document Name	

Comment	
HQ supports NPCC RSC comments and provides the following additional comments: Considering the ambiguity of the controls defined in CIP-005 5 and CIP-007 the updated version of Table R1, part 1.1 deteriorates the cyber security of the cyber assets,. The Measures column contains more explicit examples than the requirement themselves. As an example, for CIP-007 the requirement is “Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.”. The column Measures of CIP-007 R1.1 contains the following : • Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) The SDT should ensure that controls are clearly defined in CIP-005 and CIP-007 .The SDT should also ensure that the requirements are easy measurable, and limit interpretations. The suggested version of requirement 1.3 is defining the applicability by listing the following components; the operating systems, firmware, software, or software patches In the previous version of this requirement, the applicability was 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; and 1.1.5. Any security patches applied. The SDT should evaluate if the intent, of the new version, was it to increase the scope of the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see the response to NPCC RSC comments. The SDT maintains the shift from prescriptive requirements to objective level requirements is necessary to enable the standards for virtualization, as well as to permit new and emerging technologies, features and tools moving into the future. Because this approach was built with backwards compatibility in mind, entities may continue to implement a baseline as their process for changes that must be authorized. The SDT maintains the adjustments	

to Requirement R1 Part 1.3 do not increase scope, but rather reframe the existing obligation without the use of the term baseline. This is supports enabling the standard for virtualization. For this reason, the SDT did not revert nor modify the proposed requirement language.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
The new language in CIP-010 has become more complex adding to compliance risk. Additionally, CIP-010 R2 may become harder to monitor and some of the configurations required to be monitored may require new tools than the current baseline monitoring tools.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT maintains the shift from prescriptive requirements to objective level requirements is necessary to enable the standards for virtualization, as well as to permit new and emerging technologies, features and tools moving into the future. Because this approach was built with backwards compatibility in mind, entities may continue to implement a baseline as their process for changes that must be authorized. The SDT's intent when using the 'per system capability' language is to keep the scope of R2 to those things for which automated solutions are available and likely monitoring these areas and alerting entities to changes. It should be noted that the 'system' in 'per system capability' refers to the Applicable Systems for the requirement, and not the capability of the automated tool used to monitor. As a result, the 'per system capability' language does not absolve entities of the obligation to implement monitoring methods where automated solutions have not been implemented, and while potentially less ideal, manual methods to accomplish the same results where automated monitoring cannot be done remains a requirement where the Applicable System is capable of producing data related to the list of seven cyber security-related categories to monitor.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No

Document Name	
Comment	
The new language in CIP-010 has become more complex adding to compliance risk. Additionally, CIP-010 R2 may become harder to monitor and some of the configurations required to be monitored may require new tools than the current baseline monitoring tools.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT appreciates the perspective shared and maintains the shift from prescriptive requirements to objective level requirements is necessary to enable the standards for virtualization, as well as to permit new and emerging technologies, features and tools moving into the future. For this reason, the SDT did not modify the requirement language.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	
Please clarify if the change management approach or objective is shifting from change managing a device configuration to change managing a "policy" or process approach. The confusion is if the shift of focus is from managing assets determined by CIP 2 criteria towards Responsible Entity methods / processes / "policy" based documented plan. Example would be dealing with planned patch management (based on schedule or plan). If the patch does not impact CIP 5 or CIP 7 security controls, does change management only apply from a deviation of the patch management plan / policy? Suggest adding the concept of intent or "intended changes" into R1.1 and R1.4, otherwise R1.4 becomes a defacto full vulnerability assessment for any change Suggest	

R1.1 *Authorize intended changes that affect Applicable Systems where those intended changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.* *R1.4* As a part of the intended changes authorized per Part 1.1, verify that the behavior(s) any cyber security controls that were intentionally altered, or previously assessed as potentially being altered, were not adversely affected.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The change management approach is not shifting from a Cyber Asset approach to a policy-based approach. The SDT performed a comprehensive analysis of CIP-005 and CIP-007 and determined the administrative documentation (policy, plan, process, procedure etc.) requirements exist at the parent requirement level, and the implemented cyber security controls at the Cyber System or Cyber Asset level exist in the Requirement Parts. To ensure clarity that the objective is to manage configuration changes to the Applicable Systems themselves, the SDT intentionally used the language, "...serving one or more requirement parts in CIP-005 or CIP-007..." Regarding the concept of intended changes for requirement parts 1.1 and 1.4, it is the responsible entity that defines the process under R1, and that process would include those altered cyber security controls identified through execution of requirement part 1.1. The SDT determined the act of establishing the documented process defined by the Responsible Entity assures the process scope is related to intended changes, and therefore obviating the need to modify the requirement language to include 'intent'. Similarly, requirement part 1.4 is scoped to that applicable to requirement part 1.1, also addressing the concern of 'intent'.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	

Comment	
OPG supports NPCC Regional Standards Committee's comments. Please clarify if the change management approach or objective is shifting from change managing a device configuration to change managing a "policy" or process approach. The confusion is if the shift of focus is from managing assets determined by CIP 2 criteria towards Responsible Entity methods / processes / "policy" based documented plan. Example would be dealing with planned patch management (based on schedule or plan). If the patch does not impact CIP 5 or CIP 7 security controls, does change management only apply from a deviation of the patch management plan / policy? Suggest adding the concept of intent or "intended changes" into R1.1 and R1.4, otherwise R1.4 becomes a defacto full vulnerability assessment for any change Suggest R1.1 Authorize intended changes that affect Applicable Systems where those intended changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity. R1.4 As a part of the intended changes authorized per Part 1.1, verify that the behavior(s) any cyber security controls that were intentionally altered, or previously assessed as potentially being altered, were not adversely affected.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please also refer to the SDT response for NPCC RSC.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	

NST is unpersuaded by the SDT's argument that in modern computing environments, configuration baselines are of sufficiently limited value, while also being burdensome to maintain, that they can quite reasonably be downgraded from being included in CIP-010 requirements, and instead offered as merely one possible approach to compliance. Establishing and maintaining configuration baselines are identified as key elements of any good cyber security program in several NIST publications, including recently released SP 800-82 Release 3 ("Guide to Operational Technology (OT) Security") and the one cited by the SDT in its most recent Technical Justification document. Given the long-standing enthusiasm among both FERC and NERC personnel for examining and enhancing the mapping between CIP and NIST Standards, dropping a requirement to maintain documented configuration baselines seems oddly out of step with that and other related initiatives.

Regarding R1.1, it is NST's opinion that if the proposed language was adopted, there would be no end to arguments between Responsible Entities and Regional Entity audit teams about whether compliance had been adequately demonstrated. There are many possible changes to a Cyber Asset's installed software, such as security patches for data packet handlers, that would have no impact on the behavior of CIP-005 or CIP-007 controls. Should changes of this nature be exempt from a requirement to formally authorize them? NST is also concerned that allowing Responsible Entities to define the specific CIP-005 and CIP-007 controls within the scope of R1.1 could result in significant disparities among Responsible Entities and/or Regions in how these controls are identified. NST agrees CIP requirements should be written in a manner that avoids making them overly prescriptive, but at a time when NERC is seeking to impose greater consistency on Entities' CIP-008 programs (universal "attempts to compromise" criteria), it seems counterintuitive for a drafting team to be proposing changes to CIP-010 that would, in our opinion, reduce consistency.

Regarding R2.1:

NST notes that CIP-005 controls are omitted. We presume this to have been an oversight.

NST considers the proposed list of monitored items to be reasonable, but as with R1.1, we believe that it's a mistake to limit the scope to only those changes that could impact CIP-005 or CIP-007 controls, and that allowing Entities to decide on their own what they'll monitor could lead to many and varied interpretations of what R2.1 is intended to require. For example, 2.1.3 specifies monitoring for unauthorized "Installation, removal, and update of operating system, firmware, software, and cyber security patches." As noted previously, many such changes wouldn't alter CIP-005 and/or CIP-007 controls. Would it be permissible for an Entity to not consider 2.1.3 at all unless changes to a Cyber Asset's CIP-005 and/or CIP-007 behavior is detected?

Likes 0	

Dislikes 0	

Response

Thank you for your comments. The SDT maintains the shift from prescriptive requirements to objective level requirements is necessary to enable the standards for virtualization, as well as to permit new and emerging technologies, features and tools moving into the future. Because this approach was built with backwards compatibility in mind, entities may continue to implement a baseline as their process for changes that must be authorized.

The scoping of Requirement R2 is an intentional subset of the scope for Requirement R1. The focus of CIP-010-5 Requirement R1 is authorizing changes that affect the security posture of those Applicable Systems as well as the logical environments that protect them. This is why R1 includes the obligation to authorize changes that alter the behavior of one or more cyber security controls that are implemented to protect the system or environment. The Applicable Systems for the R2 monitoring requirement for unauthorized changes is an intentional a subset of cyber security controls (CIP-007) to align with the Appliable Systems scope and those technical controls that have been implemented at the System or Cyber Asset level to maintain that cyber security posture.

In Requirement R2 Part 2.1 the SDT's intention is to scope the monitoring to the seven listed items, per system capability. Additionally, the SDT also added "per system capability" in recognition that not all changes in scope can be monitored on every potential in-scope Cyber System. This addition makes the requirement conditional if a system is incapable of monitoring a particular unauthorized change category. The SDT has used the phrasing "that include at least one cyber security control for each of the following" in order to allow entities to monitor a primary security control if they have multiple overlapping controls. The SDT's intent is that having multiple security controls over these categories is a good and beneficial practice where possible, and entities should not be discouraged from having more than one. This phrasing's intent is to allow the entity to choose the primary control they monitor for unauthorized change. The entity may of course do more than one, but one is required. The SDT performed and extensive analysis of the CIP-007 requirement parts, as compared to the former baseline attribute model and concluded the seven parts are a minimum set of cyber security controls (technical controls) that must be implemented and monitored for unauthorized changes to the Applicable Systems in Part 2.1.

The SDT contends it would be difficult to defend the unauthorized "Installation, removal, and update of operating system, firmware, software, and cyber security patches." would not alter the behavior of the technical controls serving CIP-007, and maintains entities would be obligated to consider and monitor for those types of changes as written. As an example, the implementation of CIP-007 Requirement R1 technically controls the disablement or prevention of unneeded routable protocol network accessibility on each Applicable System. When installing, removing, or updating operating system, firmware, software, or security patches it is reasonable to

expect those cyber security controls that were implemented to serve CIP-007 Requirement R1 cannot behave as originally implemented because the change is one in nature that would alter the previously implemented security configuration to intentionally disable or block unneeded ports, services, or accessibility via a routable protocol. Similarly, the implementation of CIP-007 Requirement R3 technically controls an Applicable System's ability to deter, detect, or prevent malicious code. Malware prevention solutions are typically software. The installation, removal, or updating of that software is likely to alter the behavior of the originally configured cyber security control implemented to serve Requirement R3, hence the approval for those changes is required and the monitoring of at least one cyber security control that could alter the behavior of the malware prevention solution is required, and so on. The language does not preclude entities from choosing to go above and beyond the minimums of the standard based on their risk tolerance. Please see the TR for additional information on the intent of each of the seven components.

Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC

Answer	No
Document Name	

Comment

Please clarify if the change management approach or objective is shifting from change managing a device configuration to change managing a "policy" or process approach. The confusion is if the shift of focus is from managing assets determined by CIP 2 criteria towards Responsible Entity methods / processes / "policy" based documented plan.
Example would be dealing with planned patch management (based on schedule or plan). If the patch does not impact CIP 5 or CIP 7 security controls, does change management only apply from a deviation of the patch management plan / policy?

Suggest adding the concept of intent or "intended changes" into R1.1 and R1.4, otherwise R1.4 becomes a defacto full vulnerability assessment for any change
Suggest
R1.1
Authorize intended changes that affect Applicable Systems where those intended changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.
R1.4

As a part of the intended changes authorized per Part 1.1, verify that the behavior(s) any cyber security controls that were intentionally altered, or previously assessed as potentially being altered, were not adversely affected.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The change management approach is not shifting from a Cyber Asset approach to a policy-based approach. The SDT performed a comprehensive analysis of CIP-005 and CIP-007 and determined the administrative documentation (policy, plan, process, procedure etc.) requirements exist at the parent requirement level, and the implemented cyber security controls at the Cyber System or Cyber Asset level exist in the Requirement Parts. To ensure clarity that the objective is to manage configuration changes to the Applicable Systems themselves, the SDT intentionally used the language, "...serving one or more requirement parts in CIP-005 or CIP-007..."

Regarding the concept of intended changes for requirement parts 1.1 and 1.4, it is the responsible entity that defines the process under R1, and that process would include those altered cyber security controls identified through execution of requirement part 1.1. The SDT determined the act of establishing the documented process defined by the Responsible Entity assures the process scope is related to intended changes, and therefore obviating the need to modify the requirement language to include 'intent'. Similarly, requirement part 1.4 is scoped to that applicable to requirement part 1.1, also addressing the concern of 'intent'.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
Document Name	

Comment

1) With the Guidelines and Technical Basis section removed from the CIP-010-5 standard and currently nothing in the Technical Rationale or Implementation documents outlining what a CIP-010-5 R3 paper based or active vulnerability assessment should contain, does the SDT plan to add any guidance for vulnerability assessments as it relates to SCI in these aforementioned documents?

2) We need to better understand the timeline, since the 30 day timeframe is no longer listed. Also need to better understand what evidence to provide for a "baseline", since the R1 has been changed. Remove the phrase "the behavior of". Justification: 1) adding "the behavior of" might make the requirement not backwards compatible 2) adding "the behavior of" could give an impression to an auditor that we need to have additional detailed testing such as penetration testing of each altered control 3) this word will cause security teams to spend a lot of time needlessly testing low-value controls rather than looking for adversaries in their networks	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 1) The SDT will be deferring to the pre-qualified organizations for the industry development of Implementation Guidance to help assure there is an owning group that can maintain it over time, and will not be adding vulnerability assessment guidance. The Guidelines and Technical Basis section was never enforceable, and remains available in former versions of the standards if an entity chooses to refer to it as guidance. 2) the construct requires the entity to perform the obligations in R1 'as a part of the change authorized in Part 1.1. This means the Registered Entity's process must account for the order of operations associated with authorized changes and the timing needed to accomplish each requirement part such that the cyber security controls remain intact as changes occur and the Applicable System(s) is(are) secure. The SDT continues to maintain the prescriptive 'baseline' concept defeats the key objective to enable the standards for virtualization through greater flexibility in the requirement (with 'baselines' as one means to achieve the objective) and the focus at an objective level of 'what' is required, instead of getting into 'how' is supported by the terminology, "as defined by the Responsible Entity." for the methods to determine which changes "...alter the behavior of one or more cyber security controls... ...serving one or more requirement parts in CIP-005 or CIP-007...", for which those changes then require authorization per Requirement R1 Part 1.1. For these reasons, the SDT chose not to modify the requirement language. The SDT brought the security objective to the forefront in Requirement R1 Part 1.1 by starting it with "Authorize changes…". Next it narrows the scope to those "that affect Applicable Systems" and the SDT made conforming changes to Applicable Systems to add SCI. The SDT considered that many entities scope their own internal change management processes this way; if a change is to or affects something in their NERC CIP	

program for medium/highs, it goes through change management. However, the requirement needs a bit more precise scoping that is accomplished with the objective language of "…altered behaviors…" to the underlying technical controls, so it doesn't include changes such as a user changing their password or desktop background, or a system log being written to hundreds of times an hour. The requirement needs a lower bound, a floor, without attempting to incorporate a prescriptive list of change types or categories. The SDT used the objective language "…where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 and CIP-007, as defined by the Responsible Entity." The intent is to bind the scope to those changes that affect the system's CIP security posture. More precisely, the intent is to set the floor of the scope to changes that alter the behavior of a cyber security control the entity uses to keep the system secure per CIP-005 and CIP-007 requirements. Please see the Technical Rationale for additional information.

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. Please also refer to the SDT response for IRC SRC.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer	Yes
Document Name	

Comment

FirstEnergy does not opposed these changes.

Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Please also refer to the SDT response for EEI.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the changes in CIP-010 regarding the updates to change management controls. They include the change behaviors as well as the excluded physical and procedural controls, serving one or more requirement parts in CIP-005 or CIP-007.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments and support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to CIP-010.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Please also refer to the SDT response for EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes to CIP-010.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Please also refer to the SDT response for EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	

Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Please also refer to the SDT response for EEI.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren supports the proposed changes to CIP-010.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments and support.	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
USV supports the comments made by NPCC RSC	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please also refer to the SDT response for NPCC RSC.	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

6. ***The SDT revised CIP-003. Do you agree with the proposed changes to these Reliability Standards? If not, please provide the basis for your disagreement and an alternate proposal*.**

Kristine Martz - Amazon Web Services - 7	
Answer	No
Document Name	
Comment	

The inclusion of "Shared Cyber Infrastructure (SCI) that supports a low impact BCS" in the applicable systems identified in CIP-003 R2, may be confusing to Responsible Entities who only have low impact BCS because the proposed SCI definition only identifies as SCI those programmable electronic devices that host or are associated with applicable systems of different impact ratings.

First, it appears that if a Responsible Entity is using infrastructure to host only low impact VCAs, the proposed SCI definition would make CIP-003-10 R2 inapplicable to such shared infrastructure.

Second, if the Responsible Entity is using SCI to host VCAs with a low impact and another different impact rating, the proposed standard suggests that the SCI (and all of its VCAs) would need to be protected at the level applicable to the impact rating of the highest impact system(s) hosted, which would apparently subject the SCI hosting a low impact BCS to the requirements for SCI hosting medium or high impact BCS, making the requirements in CIP-003-10 R2 unnecessary or redundant.

AWS encourages the Standard Drafting Team for Project 2016-02 to develop implementation guidance, include statements in the CIP-003 Technical Rationale, or other appropriate industry supporting documents, to clarify how Responsible Entities should implement the new requirements for SCI supporting low impact BCS under CIP-003 R2 given the two issues identified above.

Likes 0	
Dislikes 0	
Response	
Thank you for your comments.	

CIP-003-10 R2 states in the parent requirement that it is applicable to "...low impact BES Cyber Systems BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS...", and the SDT agrees that where shared infrastructure is serving only low impact BCS it would not meet the 2nd component of the first bullet in the SCI definition and therefore would not qualify as SCI. Having said that, in that scenario the shared infrastructure becomes a component of the low impact BCS and would remain subject to the Requirements within R2. The SDT wanted to assure entities could use SCI to host low impact BCS, and that it is permissible to host low with medium and high on the same SCI, but then the SCI itself inherits the highest requirement set based on highest impact rated host. Where SCI is supporting BES Cyber Systems of multiple impact levels, the SDT contends it is appropriate based on risk and impact to expect that SCI be protected to the highest impacted rated BCS and associated Applicable System. While CIP-003-10 R2 may be rendered moot in this particular use case, this is one of myriad use cases thereby making CIP-003-10 R2 useful and necessary to protect the remainder. The SDT will be deferring to the pre-qualified organizations for the industry development of Implementation Guidance to help assure there is an owning group that can maintain it over time.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST believes Appendix 1 Section 2 (Physical Security Controls) should include supporting SCI, if any, for consistency with other revised CIP-003 requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Appendix A for CIP-003-10 R2 inherits the applicability for parent requirement CIP-003-10 R2, which is applicable to "...low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS..."	

Ben Hammer - Western Area Power Administration - 1

Answer	No
Document Name	

Comment

The changes to CIP-003 Specifically R2 attachment 1. should be incorporated into the CIP-004, CIP-005, CIP-006, CIP-007, and CIP-010 standards, add requirements to those standards as they pertain to low impact BES Cyber systems, either to existing requirements or to new requirements. Leave CIP-003 specifically to establishing responsibility and accountability. For Section 3 part 3.1 add an and after the 1st bullet, as shown below:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS and a Cyber System(s) outside the asset containing:
    - the low impact BCS(s); or
    - the SCI that supports a low impact BCS; **and**

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The SDT considered your suggested edits and determined consolidation of low impact requirements with medium and high requirements is out of the scope of the SAR.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	
SMUD and BANC feel that inconsistent use of the word “system”, especially with regards to “per system capability” is making the High and Medium impact requirements less stringent than the Low impact requirements. We recommend changing the language to “per Cyber Asset capability”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The SDT considered your suggestion and, because of the Note in CIP-003-10 Requirement R2 that specifically excludes the obligation to have and maintain an inventory of Cyber Assets in the low impact BES Cyber System, the SDT determined “per system capability” is the appropriate option.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
CIP Virtualization Standard proposed is CIP-003-10 is not clear. Choppy jump from section 3 to section 6, need to combine. Recommend skip this version, go to or wait for CIP-003-a	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Another drafting team is working to combine Attachment 1 Sections 3 and 6. At the point wherein that proposal is approved, the change will be merged with the CIP-003-10 changes to enable for virtualization.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the proposed changes	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Please also refer to the SDT response for EEI.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments and support. Please also refer to the SDT response for EEI.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Please also refer to the SDT response for EEI.	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI supports the proposed changes made to CIP-003.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support.	
Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott	

Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Please also refer to the SDT response for EEI.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with the proposed changes to CIP-003.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Please also refer to the SDT response for EEI.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern agrees with and supports the proposed changes to CIP-003.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments and support. Please also refer to the SDT response for EEI.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy does not opposed these changes.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments and support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mike Magruder - Avista - Avista Corporation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
Answer is yes.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

7. The SDT revised the Implementation Plan to accommodate for the future enforceable date of CIP-003-9. Do you agree with the proposed Implementation Plan? If not, please provide the basis for your disagreement and an alternate proposal.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The NAGF believes that NERC needs to clarify the process and time lines for reconciliation of the multiple CIP-003 Standards Under Development and CIP-003-09 before being able to answer Question 7 accurately.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
Unintended consequences of IRA definition could increase cost of physical access controls for medium impact with IRA.	
Likes 0	
Dislikes 0	
Response	

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
Unintended consequences of IRA definition could increase cost of physical access controls for medium impact with IRA.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST's "No" on this question reflects our concerns about several proposed or revised definitions and about proposed changes to CIP-003, CIP-004, CIP-005, CIP-007, and CIP-010.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	Yes
Document Name	
Comment	
FirstEnergy does not opposed these changes.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern agrees with the revised Implementation Plan to become effective on or about April 1, 2026 or the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions.

Likes 0	
Dislikes 0	

Response

Gail Elliott - Gail Elliott On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Gail Elliott

Answer	Yes
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the revised Implementation plan as proposed.

Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is supporting EEI comments in response to this question.	
Likes 0	
Dislikes 0	
Response	

Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
AZPS supports the revised implementation plan.	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Clay Walker On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 1, 3; Maurice Paulk, Cleco Corporation, 6, 5, 1, 3; Robert Hirchak, Cleco Corporation, 6, 5, 1, 3; Stephanie Huffman, Cleco Corporation, 6, 5, 1, 3; Wayne Messina, LaGen, 4; - Clay Walker	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Anne Kronshage - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LaTroy Brumfield - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Goi, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Galloway - John Galloway On Behalf of: Michael Puscas, ISO New England, Inc., 2; - John Galloway	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ben Hammer - Western Area Power Administration - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sheila Suurmeier - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Rachel Schuldt On Behalf of: Claudine Bates, Black Hills Corporation, 5, 6, 1, 3; - Rachel Schuldt	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Josh Combs - Black Hills Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Micah Runner - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Casey Jones - Berkshire Hathaway - NV Energy - 5 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Shannon Mickens On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Shannon Mickens, Group Name SPP RTO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; Jeremy Lawson, Northern California Power Agency, 4, 6, 3, 5; Michael Whitney, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
John Daho - John Daho On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - John Daho	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Merrell, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tracy MacNicoll - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
Answer is yes.	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	

8. ***Please provide any additional comments for the SDT to consider, if desired*****.**

Kristine Martz - Amazon Web Services - 7	
Answer	
Document Name	
Comment	

AWS supports the efforts of the Project 2016-02 SDT in addressing industry comments and feedback. We understand that the proposed revisions address on-premises virtualization, though we appreciate that these changes, such as the removal of Cyber Asset references directly in requirement language, could enable further consideration of cloud technology in future standards development projects.

Should these revisions not achieve industry consensus to move forward, we encourage the SDT to consider alternatives to the standards development process to achieve the outcomes set forth in the SAR including the development of ERO endorsed implementation guidance based on the many educational resources the SDT has already created to educate industry on cyber security for virtualized environments. Additionally, we encourage NERC to develop Risk-Based Compliance Monitoring and Enforcement Program (CMEP) Practice Guides to provide direction to ERO Enterprise CMEP staff on approaches to carry out compliance monitoring and enforcement activities related to virtualization, which is already widely employed across the industry and provides a number of oprtational and cost efficiencies as well as other benefits. Clear guidance on CIP compliance for virtual assets would greatly benefit the industry and its stakeholders by allowing for compliance certainty when moving towards greater virtualization.

Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	

Comment	
ACES and it’s members would like to thank the SDT for their continued hard work.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	
Document Name	
Comment	
With the Guidelines and Technical Basis section removed from the CIP-010-5 standard and currently nothing in the Technical Rationale or Implementation documents outlining what a CIP-010-5 R3 paper based or active vulnerability assessment should contain, does the SDT plan to add any guidance for vulnerability assessments as it relates to SCI in these aforementioned documents?	
Likes 0	
Dislikes 0	
Response	
Unfortunately, CIP-010 was already modified outside of the 2016-02 project prior to opening the standard. Since this language was already removed, the SDT will not be able to reintroduce this language at this time due to the limitations in the scope of our SAR.	
Marcus Bortman – APS – Arizona Public Service Co. – 6	
Answer	

Document Name	
Comment	
No additional comments at this time.	
Likes 0	
Dislikes 0	
Response	
Thank you for your response.	
Romel Aquino – Edison International – Southern California Edison Company – 3	
Answer	
Document Name	
Comment	
See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Daniel Gacek – Exelon – 1	
Answer	
Document Name	
Comment	

Exelon supports the comments submitted by the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Teresa Krabe – Lower Colorado River Authority – 5	
Answer	
Document Name	
Comment	
None at this time.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Junji Yamaguchi – Hydro-Quebec (HQ) – 5	
Answer	
Document Name	
Comment	
The SDT added this exemption 4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations. Our understanding	

is that “communication networks” is associated with routable protocol (layer 3 of the OSI model) and that “data communication links” is associated with non- routable protocol (layer 2 of the OSI model). SDT should clarify the intent if this is not the case.

The SDT should ensure the security posture of the Cyber Assets and not only facilitating the adoption of new technology by introducing ambiguous requirements.

The SDT should evaluate the requirements against the ERT tool approach. In other words, can the requirement be evaluated with the ERT tool?

The SDT should ensure that the requirements are clear and precise and stand by themselves and that no additional reading is required (i.e., technical rationale). The technical rationale should be viewed as a rationale and not provide explanation on how to understand the requirement.

The SDT should review the requirements with the concept of applying Protection Systems definition.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Regarding the exemption language in 4.2.3.3, the SDT intended to ensure that transport devices that were not owned by the Responsible Entity would not be in scope. This is enabled by the new language in CIP-005 1.6 which allows the entity to extend and ESP beyond a single geographic location. When the Responsible Entity enables a security control, such as encryption, across networks it doesn’t own the equipment that is carrying that traffic but has no access to the data should not be considered in scope.

In terms of the ERT tools, the SDT is unable to address enforcement issues such as how the ERT tool will accommodate the new standards. The SDT assumes that the tool will be updated accordingly by NERC’s enforcement processes.

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer	
Document Name	

Comment

The CIP-004-8 R2.3, R4.1.2, R5.1, R5.2, R6.1.2, R6.3, exclusion ‘(except for medium impact without ERC)’ appears to be unnecessary considering medium impact without ERC is not an applicable system of the requirement.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. The SDT removed the language in CIP-004-8 R2.3. Please see the CIP-004 Technical Rationale for an explanation for why this exception language is necessary.

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	
Document Name	

Comment

In the draft standards there is inconsistency in the wording of section “C. Compliance | 1. Compliance Monitoring Process | 1.1. Compliance Enforcement Authority:”. The following wording is used in CIP-003-10, and is suggested for the other standards as it matches the definition in the NERC Rules of Procedures:

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with mandatory and enforceable Reliability Standards.

The following is used in CIP-004-8, CIP-005-8, CIP-007-7 and CIP-010-5

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA)

means NERC or the Regional Entity, or any entity as otherwise designated by an

Applicable Governmental Authority, in their respective roles of monitoring and/or

enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has checked all standards and made sure the compliance section complies with the current NERC Reliability Standard template.	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	
Document Name	
Comment	
Thank you for the ability to comment.	

Likes 0	
Dislikes 0	

Response

Thank you for your comment.

Nicolas Turcotte - Hydro-Quebec (HQ) - 1

Answer	
Document Name	

Comment

The SDT added this exemption 4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations. Our understanding is that “communication networks” is associated with routable protocol (layer 3 of the OSI model) and that “data communication links” is associated with non-routable protocol (layer 2 of the OSI model). SDT should clarify the intent if this is not the case.

The SDT should ensure the security posture of the Cyber Assets and not only facilitating the adoption of new technology by introducing ambiguous requirements.

The SDT should evaluate the requirements against the ERT tool approach. In other words, can the requirement be evaluated with the ERT tool?

The SDT should ensure that the requirements are clear and precise and stand by themselves and that no additional reading is required, i.e., technical rationale. The technical rationale should be viewed as a rationale and not provide explanation on how to understand the requirement.

The SDT should review the requirements with the concept of applying Protection Systems definition.

Likes 0	
Dislikes 0	

Response

Thank you for your comment. Regarding the exemption language in 4.2.3.3, the SDT intended to ensure that transport devices that were not owned by the Responsible Entity would not be in scope. This is enabled by the new language in CIP-005 1.6 which allows the entity to extend and ESP beyond a single geographic location. When the Responsible Entity enables a security control, such as encryption, across networks it doesn’t own the equipment that is carrying that traffic but has no access to the data should not be considered in scope. In terms of the ERT tools, the SDT is unable to address enforcement issues such as how the ERT tool will accommodate the new standards. The SDT assumes that the tool will be updated accordingly by NERC’s enforcement processes.	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE supports EEI comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to EEI.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Please see response to MRO NSRF.	
Ellese Murphy - Ellese Murphy On Behalf of: Marcelo Pesantez, Duke Energy - Florida Power Corporation, 3; - Ellese Murphy	
Answer	
Document Name	
Comment	
Duke Energy thanks the Virtualization Standard Drafting Team for their hard work to get to Draft 5, and for their careful consideration of industry comments from Draft 4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	
Document Name	
Comment	
In the draft standards there is inconsistency in the wording of section “C. Compliance | 1. Compliance Monitoring Process | 1.1. Compliance Enforcement Authority:”. The following wording is used in CIP-003-10, and is suggested for the other standards as it matches the definition in the NERC Rules of Procedures: **1.1. Compliance Enforcement Authority:** As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with mandatory and enforceable Reliability Standards.	

The following is used in CIP-004-8, CIP-005-8, CIP-007-7 and CIP-010-5 **1.1. Compliance Enforcement Authority:** "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT has checked all standards and made sure the compliance section complies with the current NERC Reliability Standard template.	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
CIP-005 R2.6: BPA reiterates disagreement with the requirement to prevent sharing of memory resources in R2.6. The theoretical risk represented by CPU-sharing is not high enough to mandate the significant re-architecture required to adequately separate CPU usage as specified in Part 2.6. BPA recommends allowing the continued use of shared resources to allow entities the flexibility to balance risk mitigation with resources, maintenance and cost of maintaining the grid.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comment. Based on industry feedback the SDT was trying to strike a balance between the flexibility of virtualization and known CPU/memory vulnerabilities. The intent is to allow clusters of devices such as servers to be leveraged with rules to prevent the sharing of CPU/memory. The SDT thought this was an acceptable balance to allow entities to take advantage of pooling resources while still avoiding the security risks associated with sharing CPU/memory on the same individual device.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	

Thank you for your comment.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
FirstEnergy asks the DT for clarification training requirements for CIP-004. Training requirement 2.2 and 2.3 appear to be inconsistent in the description with the use of “includes Mediums with ERC” as well as Access Authorization/verification in requirement 4.1 and 4.2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The SDT removed the language in CIP-004-8 R2.3. Please see the CIP-004 Technical Rationale for an explanation for why this exception language is necessary.	

End of Report

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reminder

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Additional Ballots and Non-binding Polls Open through November 29, 2023

Now Available

The additional ballots for draft 5 of the **CIP Virtualization standards (outlined below)** and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels are open through **8 p.m. Eastern, Wednesday, November 29, 2023**.

- CIP-003-10 - Cyber Security – Security Management Controls*
- CIP-004-8 - Cyber Security – Personnel & Training*
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments

*****_Based on recent board adopted standards for CIP-003-9 and CIP-004-7, the posted versions for the 2016-02 Modifications to CIP Standards were updated to reflect CIP-003-10 and CIP-004-8. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-9 and CIP-004-7, the version numbers within this posting are correct and entities will be voting on CIP-003-10 and CIP-004-8._

The standard drafting team's considerations of the responses received from the last comment period are reflected in these drafts of the standards.

Reminder Regarding Corporate RBB Memberships

Under the NERC Rules of Procedure, each entity and its affiliates is collectively permitted one voting membership per Registered Ballot Body Segment. Each entity that undergoes a change in corporate structure (such as a merger or acquisition) that results in the entity or affiliated entities having more than the one permitted representative in a particular Segment must withdraw the duplicate membership(s) prior to joining new ballot pools or voting on anything as part of an existing ballot pool. Contact ballotadmin@nerc.net to assist with the removal of any duplicate registrations.

Balloting

Members of the ballot pools associated with this project can log in and submit their votes by accessing the Standards Balloting and Commenting System (SBS) here.

Note: Votes cast in previous ballots will not carry over to additional ballots. It is the responsibility of the registered voter in the ballot pools to place votes again. To ensure a quorum is reached, if you do not want to vote affirmative or negative, cast an abstention.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The ballot and comment results will be announced and posted on the project page. The drafting team will review all responses received during the comment period and determine the next steps of the project.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager of Standards Development, Alison Oswald (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Formal Comment Period Open through November 16, 2023

Now Available

A formal comment period for draft 5 of the **CIP Virtualization standards (outlined below)** is open through **8 p.m. Eastern, Thursday, November 16, 2023**.

- CIP-003-10 - Cyber Security – Security Management Controls*
- CIP-004-8 - Cyber Security – Personnel & Training*
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments

*Based on recent board adopted standards for CIP-003-9 and CIP-004-7, the posted versions for the 2016-02 Modifications to CIP Standards reflect CIP-003-10 and CIP-004-8. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-9 and CIP-004-7, the version numbers within this posting are correct and entities will be voting on CIP-003-10 and CIP-004-8.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **November 7 - 16, 2023**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager of Standards Development, Alison Oswald (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Formal Comment Period Open through November 16, 2023

Now Available

A formal comment period for draft 5 of the **CIP Virtualization standards (outlined below)** is open through **8 p.m. Eastern, Thursday, November 16, 2023**.

- CIP-003-10 - Cyber Security – Security Management Controls*
- CIP-004-8 - Cyber Security – Personnel & Training*
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments

*Based on recent board adopted standards for CIP-003-9 and CIP-004-7, the posted versions for the 2016-02 Modifications to CIP Standards reflect CIP-003-10 and CIP-004-8. The Standards Balloting and Commenting System (SBS) does not allow edits once a ballot pool has been formed. Even though the standard versioning within the SBS states CIP-003-9 and CIP-004-7, the version numbers within this posting are correct and entities will be voting on CIP-003-10 and CIP-004-8.

The standard drafting team's considerations of the responses received from the previous comment period are reflected in these drafts of the standards.

Commenting

Use the Standards Balloting and Commenting System (SBS) to submit comments. An unofficial Word version of the comment form is posted on the project page.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Additional ballots for the standards and non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **November 7 - 16, 2023**.

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager of Standards Development, Alison Oswald (via email) or at (404) 446-2589. Subscribe to this project's observer mailing list by selecting "NERC Email Distribution Lists" from the "Service" drop-down menu and specify “Project 2016-02 Modifications to CIP Standards Observer List” in the Description Box.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/305)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 AB 5 ST
Voting Start Date: 11/20/2023 12:01:00 AM
Voting End Date: 11/29/2023 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 5
Total # Votes: 248
Total Ballot Pool: 298
Quorum: 83.22
Quorum Established Date: 11/29/2023 3:54:15 PM
Weighted Segment Value: 93.8

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	59	0.908	6	0.092	0	8	13
Segment: 2	8	0.5	5	0.5	0	0	0	1	2
Segment: 3	65	1	46	0.939	3	0.061	0	5	11
Segment: 4	15	1	9	0.9	1	0.1	0	1	4
Segment: 5	71	1	46	0.939	3	0.061	0	8	14
Segment: 6	44	1	33	0.943	2	0.057	0	4	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	5	0.5	0	0	0	1	1
Totals:	298	6	203	5.628	15	0.372	0	30	50

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Affirmative	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		None	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Tracy MacNicoll		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Christopher Siewert		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson	Amie Shuger McConnaha	None	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Claudine Bates		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Affirmative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 298 of 298 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/305)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 AB 5 ST
Voting Start Date: 11/20/2023 12:01:00 AM
Voting End Date: 11/29/2023 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 5
Total # Votes: 249
Total Ballot Pool: 296
Quorum: 84.12
Quorum Established Date: 11/29/2023 3:45:49 PM
Weighted Segment Value: 84.73

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	50	0.769	15	0.231	0	8	13
Segment: 2	8	0.6	6	0.6	0	0	0	0	2
Segment: 3	65	1	42	0.857	7	0.143	0	6	10
Segment: 4	14	0.9	7	0.7	2	0.2	0	2	3
Segment: 5	71	1	40	0.8	10	0.2	0	8	13
Segment: 6	43	1	30	0.857	5	0.143	0	3	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	5	0.5	0	0	0	1	1
Totals:	296	6	180	5.084	39	0.916	0	30	47

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Negative	Comments Submitted
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer		Negative	Comments Submitted
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Affirmative	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Tracy MacNicoll		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Christopher Siewert		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/305)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 AB 5 ST
Voting Start Date: 11/20/2023 12:01:00 AM
Voting End Date: 11/29/2023 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 5
Total # Votes: 249
Total Ballot Pool: 295
Quorum: 84.41
Quorum Established Date: 11/29/2023 3:45:06 PM
Weighted Segment Value: 72.73

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	45	0.692	20	0.308	0	8	12
Segment: 2	8	0.6	5	0.5	1	0.1	0	0	2
Segment: 3	65	1	37	0.771	11	0.229	0	7	10
Segment: 4	14	0.8	5	0.5	3	0.3	0	3	3
Segment: 5	71	1	36	0.72	14	0.28	0	8	13
Segment: 6	43	1	25	0.735	9	0.265	0	4	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.4	3	0.3	1	0.1	0	2	1
Totals:	295	5.8	156	4.218	59	1.582	0	34	46

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	Third-Party Comments
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Negative	Comments Submitted
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer		Negative	Comments Submitted
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Negative	Comments Submitted
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Tracy MacNicoll		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Abstain	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Christopher Siewert		Negative	Comments Submitted
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Negative	Comments Submitted
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	WEC Energy Group, Inc.	Michelle Hribar		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Great River Energy	Brian Meloy		None	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Negative	Comments Submitted
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 295 of 295 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/305)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 AB 5 ST
Voting Start Date: 11/20/2023 12:01:00 AM
Voting End Date: 11/29/2023 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 5
Total # Votes: 249
Total Ballot Pool: 295
Quorum: 84.41
Quorum Established Date: 11/29/2023 3:44:55 PM
Weighted Segment Value: 89.32

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	56	0.862	9	0.138	0	8	12
Segment: 2	8	0.6	5	0.5	1	0.1	0	0	2
Segment: 3	65	1	44	0.917	4	0.083	0	7	10
Segment: 4	14	0.8	7	0.7	1	0.1	0	3	3
Segment: 5	71	1	44	0.88	6	0.12	0	8	13
Segment: 6	43	1	31	0.912	3	0.088	0	4	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.5	5	0.5	0	0	0	1	1
Totals:	295	5.9	192	5.27	24	0.63	0	33	46

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Affirmative	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Tracy MacNicoll		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Abstain	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Christopher Siewert		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Michelle Hribar		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Affirmative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 295 of 295 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/305)
Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 AB 5 ST
Voting Start Date: 11/20/2023 12:01:00 AM
Voting End Date: 11/29/2023 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 5
Total # Votes: 250
Total Ballot Pool: 295
Quorum: 84.75
Quorum Established Date: 11/29/2023 3:44:44 PM
Weighted Segment Value: 74.46

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	85	1	49	0.766	15	0.234	0	9	12
Segment: 2	8	0.6	2	0.2	4	0.4	0	0	2
Segment: 3	65	1	40	0.833	8	0.167	0	7	10
Segment: 4	14	0.8	7	0.7	1	0.1	0	3	3
Segment: 5	71	1	38	0.745	13	0.255	0	7	13
Segment: 6	43	1	28	0.824	6	0.176	0	4	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 9	0	0	0	0	0	0	0	0	0
Segment: 10	7	0.6	4	0.4	2	0.2	0	1	0
Totals:	295	6	168	4.468	49	1.532	0	33	45

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	LaTroy Brumfield		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Third-Party Comments
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	Third-Party Comments
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Third-Party Comments
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Abstain	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	Third-Party Comments
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Negative	Comments Submitted
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		Negative	Third-Party Comments
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	Third-Party Comments
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Tracy MacNicoll		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Christopher Siewert		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cowlitz County PUD	Deanna Carlson		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	Third-Party Comments
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	Third-Party Comments
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Third-Party Comments
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Michelle Hribar		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	Third-Party Comments
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Kristine Martz		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 295 of 295 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 | Non-binding Poll AB 5 NB
Voting Start Date: 11/20/2023 12:01:00 AM
Voting End Date: 11/29/2023 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 5
Total # Votes: 223
Total Ballot Pool: 272
Quorum: 81.99
Quorum Established Date: 11/29/2023 4:11:49 PM
Weighted Segment Value: 92.61

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	45	0.882	6	0.118	16	12
Segment: 2	8	0.4	4	0.4	0	0	2	2
Segment: 3	62	1	41	0.953	2	0.047	8	11
Segment: 4	14	1	9	0.9	1	0.1	1	3
Segment: 5	62	1	36	0.947	2	0.053	11	13
Segment: 6	39	1	24	0.923	2	0.077	6	7
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	4	0.4	0	0	2	1
Totals:	272	5.8	163	5.406	13	0.394	47	49

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Salt River Project	Sarah Blankenship	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Affirmative	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		None	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Affirmative	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Tracy MacNicoll		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Christopher Siewert		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Affirmative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 272 of 272 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 | Non-binding Poll AB 5 NB
Voting Start Date: 11/20/2023 12:01:00 AM
Voting End Date: 11/29/2023 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 5
Total # Votes: 225
Total Ballot Pool: 272
Quorum: 82.72
Quorum Established Date: 11/29/2023 4:06:24 PM
Weighted Segment Value: 81.03

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	38	0.76	12	0.24	17	12
Segment: 2	8	0.5	5	0.5	0	0	1	2
Segment: 3	62	1	36	0.857	6	0.143	10	10
Segment: 4	14	0.9	7	0.7	2	0.2	2	3
Segment: 5	62	1	30	0.789	8	0.211	12	12
Segment: 6	39	1	21	0.808	5	0.192	6	7
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	4	0.4	0	0	2	1
Totals:	272	5.8	141	4.814	33	0.986	51	47

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Abstain	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer		Negative	Comments Submitted
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Affirmative	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Abstain	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Tracy MacNicoll		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Christopher Siewert		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	New York Power Authority	Shelly Dineen		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 272 of 272 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 | Non-binding Poll AB 5 NB
Voting Start Date: 11/20/2023 12:01:00 AM
Voting End Date: 11/29/2023 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 5
Total # Votes: 225
Total Ballot Pool: 272
Quorum: 82.72
Quorum Established Date: 11/29/2023 4:06:02 PM
Weighted Segment Value: 70.18

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	79	1	34	0.68	16	0.32	17	12
Segment: 2	8	0.5	4	0.4	1	0.1	1	2
Segment: 3	62	1	31	0.756	10	0.244	11	10
Segment: 4	14	0.8	5	0.5	3	0.3	3	3
Segment: 5	62	1	27	0.711	11	0.289	12	12
Segment: 6	39	1	17	0.68	8	0.32	7	7
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	2	0.2	2	0.2	2	1
Totals:	272	5.7	120	3.927	51	1.773	54	47

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Negative	Comments Submitted
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	Comments Submitted
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Abstain	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Abstain	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Negative	Comments Submitted
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer		Negative	Comments Submitted
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Negative	Comments Submitted
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Abstain	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Tracy MacNicoll		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Abstain	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Christopher Siewert		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	Comments Submitted
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	Comments Submitted
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	New York Power Authority	Shelly Dineen		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 272 of 272 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 | Non-binding Poll AB 5 NB
Voting Start Date: 11/20/2023 12:01:00 AM
Voting End Date: 11/29/2023 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 5
Total # Votes: 224
Total Ballot Pool: 273
Quorum: 82.05
Quorum Established Date: 11/29/2023 4:21:15 PM
Weighted Segment Value: 87.79

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	44	0.846	8	0.154	15	13
Segment: 2	8	0.4	3	0.3	1	0.1	2	2
Segment: 3	62	1	38	0.927	3	0.073	10	11
Segment: 4	14	0.8	7	0.7	1	0.1	3	3
Segment: 5	62	1	33	0.868	5	0.132	12	12
Segment: 6	39	1	22	0.88	3	0.12	7	7
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.4	4	0.4	0	0	2	1
Totals:	273	5.6	151	4.921	21	0.679	52	49

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Affirmative	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		None	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Tracy MacNicoll		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Abstain	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Christopher Siewert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Affirmative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 273 of 273 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 | Non-binding Poll AB 5 NB
Voting Start Date: 11/20/2023 12:01:00 AM
Voting End Date: 11/29/2023 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 5
Total # Votes: 226
Total Ballot Pool: 273
Quorum: 82.78
Quorum Established Date: 11/29/2023 4:05:15 PM
Weighted Segment Value: 75.14

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	80	1	39	0.75	13	0.25	15	13
Segment: 2	8	0.4	1	0.1	3	0.3	2	2
Segment: 3	62	1	34	0.829	7	0.171	11	10
Segment: 4	14	0.8	7	0.7	1	0.1	3	3
Segment: 5	62	1	27	0.711	11	0.289	12	12
Segment: 6	39	1	19	0.76	6	0.24	7	7
Segment: 7	0	0	0	0	0	0	0	0
Segment: 8	1	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 10	7	0.5	3	0.3	2	0.2	2	0
Totals:	273	5.7	130	4.15	43	1.55	53	47

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Abstain	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		None	N/A
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	Comments Submitted
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	Comments Submitted
1	Entergy	Brian Lindsey		Negative	Comments Submitted
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Glencoe Light and Power Commission	Terry Volkmann		Abstain	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Abstain	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	NB Power Corporation	Jeffrey Streifling		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	Comments Submitted
1	New York Power Authority	Daniel Valle		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Steve Toosevich		Negative	Comments Submitted
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Abstain	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		None	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	Comments Submitted
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		Abstain	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Abstain	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Bobbi Welch		Abstain	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Abstain	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Negative	Comments Submitted
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Abstain	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Abstain	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A
3	Lincoln Electric System	Sam Christensen		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Los Angeles Department of Water and Power	Tony Skourtas		Abstain	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		None	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	Comments Submitted
3	Salt River Project	Mathew Weber	Israel Perez	Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	Marc Sedor		None	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		None	N/A
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	Comments Submitted
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Tracy MacNicoll		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Abstain	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Christopher Siewert		Affirmative	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	Comments Submitted
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	Comments Submitted
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Abstain	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Negative	Comments Submitted
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Abstain	N/A
5	New York Power Authority	Zahid Qayyum		Negative	Comments Submitted
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	Comments Submitted
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	Comments Submitted
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Abstain	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		None	N/A
5	PSEG Nuclear LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	Comments Submitted
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Melanie Wong		None	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		None	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Michael Foley		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joseph OBrien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	Comments Submitted
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	Comments Submitted
6	Salt River Project	Timothy Singh	Israel Perez	Negative	Comments Submitted
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		None	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Lindsey Mannion		Negative	Comments Submitted
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Negative	Comments Submitted
10	Western Electricity Coordinating Council	Steven Rueckert		Abstain	N/A

Previous 1 Next

Showing 1 to 273 of 273 entries

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 – 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 CIP Definitions”

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-7

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BCS could have on the reliable operation of the Bulk Electric System (BES). Identification and categorization of BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. **Balancing Authority**

   4.1.2. **Distribution Provider that owns** one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-7:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of Parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** RAS that support the reliable operation of the BES; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer of identified BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent but less than or equal to 10 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category;	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BCS, more than 10 percent but less than or equal to 15 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category;	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of identified BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more

R #	Violation Severity Levels (CIP-002-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	fewer identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, five percent or fewer high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, five or fewer high or medium BCS have not been identified.	OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than five percent but less than or equal to 10 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than five but less than or equal to 10 high or medium BCS have not been identified.	OR For Responsible Entities with a total of 100 or fewer high or medium impact BCS, more than 10 but less than or equal to 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 10 percent but less than or equal to 15 percent high or medium BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BCS, more than 10 but less than or equal to 15 high or medium BCS have not been identified.	than 15 identified BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BCS, more than 15 percent of high or medium impact BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BCS have not been identified.
R2	The Responsible Entity did not complete its review and update	The Responsible Entity did not complete its review and update	The Responsible Entity did not complete its review and update	The Responsible Entity did not complete its review and update

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-002-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (Part 2.1)
OR
The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (Part 2.2)</td><td>for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (Part2.1)
OR
The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (Part 2.2)</td><td>for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (Part 2.1)
OR
The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (Part 2.2)</td><td>for the identification required for Requirement R1 within 18 calendar months of the previous review. (Part 2.1)
OR
The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (Part 2.2)</td></tr>
</table>

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-002-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
7	TBD	Virtualization Modifications	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High impact rating**

   Each BCS used by and located at any of the following:

   1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

   1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

   1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

   1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium impact rating**

   Each BCS, not included in Section 1 above, associated with any of the following:

   2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

   2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

   2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

   2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

   2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each RAS or automated switching System that operates BES Elements, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in high impact rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in high impact rating, above.

2.13. Each Control Center or backup Control Center, not already included in high impact rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low impact rating

BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 – 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 ~~Draft 4~~CIP Definitions”

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-~~6~~7

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES

4. Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those ~~BES Cyber Systems~~BCS could have on the reliable operation of the ~~BES.~~Bulk Electric System (BES). Identification and categorization of ~~BES Cyber Systems~~BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

5. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and

including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each ~~Remedial Action Scheme~~RAS where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-~~6~~7:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective ~~Date~~Dates: See “Project 2016-02 Modifications to CIP Standards Implementation Plan ~~for CIP-002-6.~~”

~~**6. Background:** This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~**BES Cyber Systems**~~

~~The CIP Cyber Security Standards use the “BES Cyber System” term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.~~

~~Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.~~

~~It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Reliable Operation of the BES~~

~~The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.~~

~~Real-time Operations~~

~~One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.~~

~~Categorization Criteria~~

~~The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement R1 only requires the discrete identification of BES~~

~~Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact.~~

~~This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the CIP Cyber Security Standards.~~

~~Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems~~

~~BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:~~

- **~~Electronic Access Control or Monitoring Systems (“EACMS”) –~~** ~~Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.~~
- **~~Physical Access Control Systems (“PACS”) –~~** ~~Examples include: authentication servers, card systems, and badge control systems.~~
- **~~Protected Cyber Assets (“PCA”) –~~** ~~Examples include, to the extent they are within the ESP: file servers, FTP servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of ~~parts~~Parts 1.1 through 1.3: *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;

ii. Transmission stations and substations;

iii. Generation resources;

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;

v. ~~Remedial Action Schemes~~RAS that support the reliable operation of the ~~Bulk Electric System~~BES; and

vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact ~~BES Cyber System~~BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact ~~BES Cyber System~~BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact ~~BES Cyber System~~BCS according to Attachment 1, Section 3, if any (a discrete list of low impact ~~BES Cyber Systems~~BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1~~, and Parts 1.1 and 1.2.~~.

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1~~.~~ Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2~~.~~ Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention ~~period(s)~~periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program:

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~**1.1. Additional Compliance Information:**~~

~~None.~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-002-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1~~.~~	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, five percent or fewer of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than five percent but less than or equal to 10 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact ~~BES Cyber Systems~~BCS, more than 10 percent but less than or equal to 15 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 15 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and

R #	Violation Severity Levels (CIP-002-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	medium impact ~~BES Cyber Systems~~BCS, five or fewer identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, five percent or fewer high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, five or fewer high or medium ~~BES Cyber Systems~~BCS have not been identified.	incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact~~ and BES Cyber Systems~~BCS, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than five percent but less than or equal to 10 percent high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than five	incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact ~~and BES Cyber Assets~~BCS, more than 10 but less than or equal to 15 identified ~~BES Cyber Assets~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 10 percent but less than or equal to 15 percent high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than 10 but	medium impact ~~BES Cyber Systems~~BCS, more than 15 identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 15 percent of high or medium impact ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact ~~BES Cyber Systems~~BCS have not been identified.

R #	Violation Severity Levels (CIP-002-~~6~~7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
		but less than or equal to 10 high or medium ~~BES Cyber Systems~~BCS have not been identified.	less than or equal to 15 high or medium ~~BES Cyber Systems~~BCS have not been identified.	
R2~~.~~	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (~~R2~~Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (~~R2~~Part 2.2)	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (~~R2~~Part2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (~~R2~~Part 2.2)	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (~~R2~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (~~R2~~Part 2.2)	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (~~R2~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (~~R2~~Part 2.2)

D. Regional Variances

None.

E. Interpretations

None.

~~E.~~F. Associated Documents

- ~~See~~ Implementation Plan for ~~CIP-002-6~~Project 2016-02~~.~~
- ~~See Appendix 1. The Interpretation in Appendix 1 was developed under a prior version of the Reliability Standard,~~ CIP-002-7 Technical Rationale~~5.1, and is being carried forward to subsequent versions.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update

Version	Date	Action	Change Tracking
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
7	TBD	Virtualization Modifications	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High ~~Impact Rating~~impact rating

Each ~~BES Cyber System~~BCS used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4~~.~~ Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium ~~Impact Rating~~impact rating

Each ~~BES Cyber System~~BCS, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each ~~Remedial Action Scheme (~~RAS~~)~~ or automated switching System that operates BES Elements, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding

(UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in ~~High Impact Rating~~high impact rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center~~, not included in the High Impact Rating,~~ used to perform the ~~reliability tasks~~functional obligations of ~~a~~the Transmission Operator ~~in real-time to monitor and control BES Transmission Lines with an "aggregate weighted value" exceeding 6000 according to the table below. The "aggregate weighted value" for a Control Center or backup Control Center is determined by summing the "weight value per line" shown in the table below for each BES Transmission Line monitored and controlled by the Control Center or backup Control Center~~not included in high impact rating, above.

2.13. Each Control Center or backup Control Center, not already included in ~~High Impact Rating~~high impact rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low ~~Impact Rating~~impact rating

~~BES Cyber Systems~~BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. ~~Remedial Action Schemes~~RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-6 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.~~

~~For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-6. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.~~

~~CIP-002-6~~

~~CIP-002-6 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, “…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES.”~~

~~The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-6. The concept includes a number of named BES reliability operating services. These named services include:~~

- ~~Dynamic Response to BES conditions~~

- ~~Balancing Load and Generation~~
- ~~Controlling Frequency (Real Power)~~
- ~~Controlling Voltage (Reactive Power)~~
- ~~Managing Constraints~~
- ~~Monitoring & Control~~
- ~~Restoration of BES~~
- ~~Situational Awareness~~
- ~~Inter-Entity Real-Time Coordination and Communication~~

~~Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.~~

~~Entity Registration~~	~~RC~~	~~BA~~	~~TOP~~	~~TO~~	~~DP~~	~~GOP~~	~~GO~~
~~Dynamic Response~~		~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Balancing Load & Generation~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Controlling Frequency~~		~~X~~				~~X~~	~~X~~
~~Controlling Voltage~~			~~X~~	~~X~~	~~X~~		~~X~~
~~Managing Constraints~~	~~X~~		~~X~~			~~X~~	
~~Monitoring and Control~~			~~X~~			~~X~~	
~~Restoration~~			~~X~~			~~X~~	
~~Situation Awareness~~	~~X~~	~~X~~	~~X~~			~~X~~	
~~Inter-Entity coordination~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~	~~X~~

~~Dynamic Response~~

~~The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:~~

- ~~Spinning reserves (contingency reserves)~~
    - ~~Providing actual reserve generation when called upon (GO,GOP)~~
    - ~~Monitoring that reserves are sufficient (BA)~~
- ~~Governor Response~~
    - ~~Control system used to actuate governor response (GO)~~
- ~~Protection Systems (transmission & generation)~~
    - ~~Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)~~
    - ~~Zone protection for breaker failure (DP, TO, TOP)~~
    - ~~Breaker protection (DP, TO, TOP)~~
    - ~~Current, frequency, speed, phase (TO,TOP, GO,GOP)~~
- ~~Remedial Action Schemes~~
    - ~~Sensors, relays, and breakers, possibly software (DP, TO, TOP)~~
- ~~Under and Over Frequency relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Under and Over Voltage relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Power System Stabilizers (GO)~~

~~Balancing Load and Generation~~

~~The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:~~

- ~~Calculation of Area Control Error (ACE)~~
    - ~~Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)~~
    - ~~Software used to perform calculation (BA)~~
- ~~Demand Response~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP,DP)~~
- ~~Manually Initiated Load shedding~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP, DP)~~
- ~~Non-spinning reserve (contingency reserve)~~

  - ~~Know generation status, capability, ramp rate, start time (GO, BA)~~
  - ~~Start units and provide energy (GOP)~~

~~Controlling Frequency (Real Power)~~

~~The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:~~

- ~~Generation Control (such as AGC)~~
  - ~~ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)~~
  - ~~Software to calculate unit adjustments (BA)~~
  - ~~Transmit adjustments to individual units (GOP)~~
  - ~~Unit controls implementing adjustments (GOP)~~
- ~~Regulation (regulating reserves)~~
  - ~~Frequency source, schedule (BA)~~
  - ~~Governor control system (GO)~~

~~Controlling Voltage (Reactive Power)~~

~~The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:~~

- ~~Automatic Voltage Regulation (AVR)~~
  - ~~Sensors, stator control system, feedback (GO)~~
- ~~Capacitive resources~~
  - ~~Status, control (manual or auto), feedback (TOP, TO,DP)~~
- ~~Inductive resources (transformer tap changer, or inductors)~~
  - ~~Status, control (manual or auto), feedback (TOP,TO,DP)~~
- ~~Static VAR Compensators (SVC)~~
  - ~~Status, computations, control (manual or auto), feedback (TOP, TO,DP)~~

~~Managing Constraints~~

~~Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:~~

- ~~Available Transfer Capability (ATC) (TOP)~~

- ~~Interchange schedules (TOP, RC)~~
- ~~Generation re-dispatch and unit commit (GOP)~~
- ~~Identify and monitor SOL's & IROL's (TOP, RC)~~
- ~~Identify and monitor Flow gates (TOP, RC)~~

~~Monitoring and Control~~

~~Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:~~

- ~~All methods of operating breakers and switches~~
  - ~~SCADA (TOP, GOP)~~
  - ~~Substation automation (TOP)~~

~~Restoration of BES~~

~~The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:~~

- ~~Restoration including planned cranking path~~
  - ~~Through black start units (TOP, GOP)~~
  - ~~Through tie lines (TOP, GOP)~~
- ~~Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)~~
- ~~Coordination (TOP, TO, BA, RC, DP, GO, GOP)~~

~~Situational Awareness~~

~~The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:~~

- ~~Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)~~
- ~~Change management (TOP,GOP,RC,BA)~~
- ~~Current Day and Next Day planning (TOP)~~
- ~~Contingency Analysis (RC)~~
- ~~Frequency monitoring (BA, RC)~~

~~Inter-Entity Coordination~~

~~The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and~~

~~operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:~~

- ~~Scheduled interchange (BA,TOP,GOP,RC)~~
- ~~Facility operational data and status (TO, TOP, GO, GOP, RC, BA)~~
- ~~Operational directives (TOP, RC, BA)~~

~~Applicability to Distribution Providers~~

~~It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.~~

~~Requirement R1:~~

~~Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.~~

~~Attachment 1~~

~~Overall Application~~

~~In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.~~

~~When the drafting team uses the term “Facilities,” there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as, “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-6, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may~~

~~be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.~~

~~In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.~~

~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.~~

~~High Impact Rating~~

~~This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.~~

~~The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.~~

~~Additional thresholds as specified in the criteria apply for this category.~~

~~Medium Impact Rating~~

~~No additional evaluation is necessary for BES Cyber Systems that have already been identified as high impact.~~

~~***Generation***~~

~~The criteria in Attachment 1’s medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.~~

- ~~Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is “to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance.” In particular, it requires that “as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency.” The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.~~

  ~~In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.~~

  ~~By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.~~

  ~~The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities’ qualification against these bright-lines, the highest value was used.~~

- ~~In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a “long term” reliability planning, i.e. that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as “Reliability Must Run,” and this designation is distinct from those generation Facilities designated as “must run” for market stabilization purposes. Because the use of the term “must run” creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units~~

~~designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.~~

~~If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.~~

~~The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.~~

- ~~Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~

  ~~IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.~~

- ~~Criterion 2.9 categorizes BES Cyber Systems for Remedial Action Schemes as medium impact. Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.~~

- ~~Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.~~

- ~~Criterion 2.13 categorizes as medium impact those BA Control Centers that “control” 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~***Transmission***~~

~~*The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical*~~

~~borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.~~

- ~~Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.~~
- ~~Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.~~

  ~~It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.~~
- ~~Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:~~
    - ~~Excluded radial facilities that would only provide support for single generation facilities.~~
    - ~~Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.~~

  ~~The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.~~

~~Additionally, in Attachment 1 of NERC's "Integrated Risk Assessment Approach – Refinement to Severity Risk Index" document, the report used an average MVA line loading based on kV rating:~~

- ~~230 kV –> 700 MVA~~
- ~~345 kV –> 1,300 MVA~~
- ~~500 kV –> 2,000 MVA~~
- ~~765 kV –> 3,000 MVA~~

~~In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:~~

- ~~For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.~~
- ~~Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~
- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

  ~~Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.~~

  1. ~~The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.~~

2. ~~The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4.: there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.~~

~~The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.~~

- ~~Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~
- ~~Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.~~
- ~~Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.~~
- ~~Criterion 2.9 designates as medium impact those BES Cyber Systems for those Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.~~
- ~~Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted~~

~~that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.~~

~~This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.~~

~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.~~

- ~~Criterion 2.12 categorizes medium impact BES Cyber Systems associated with Control Centers and backup Control Centers, including associated data centers, that monitor and control BES Transmission Lines with an aggregate weighted value of 6000 or higher, and that have not already been included in Part 1. The drafting team included additional qualifications in this criterion that would ensure the required level of impact to the BES is defined and a risk threshold associated to establish a floor for applicable medium impact BES Cyber Systems.~~

  ~~The total aggregated weighted value is used to account for the impact to the BES. The 6000 aggregate weighted value threshold defined in criterion 2.12 provides a sufficient differentiation for medium and low impact BES Cyber Systems associated with Control Centers that monitor and control BES Transmission Lines. SDT analysis of Transmission Control Centers validated that those facilities that may have significant impact are categorized at an appropriate level commensurate with the associated risk.~~

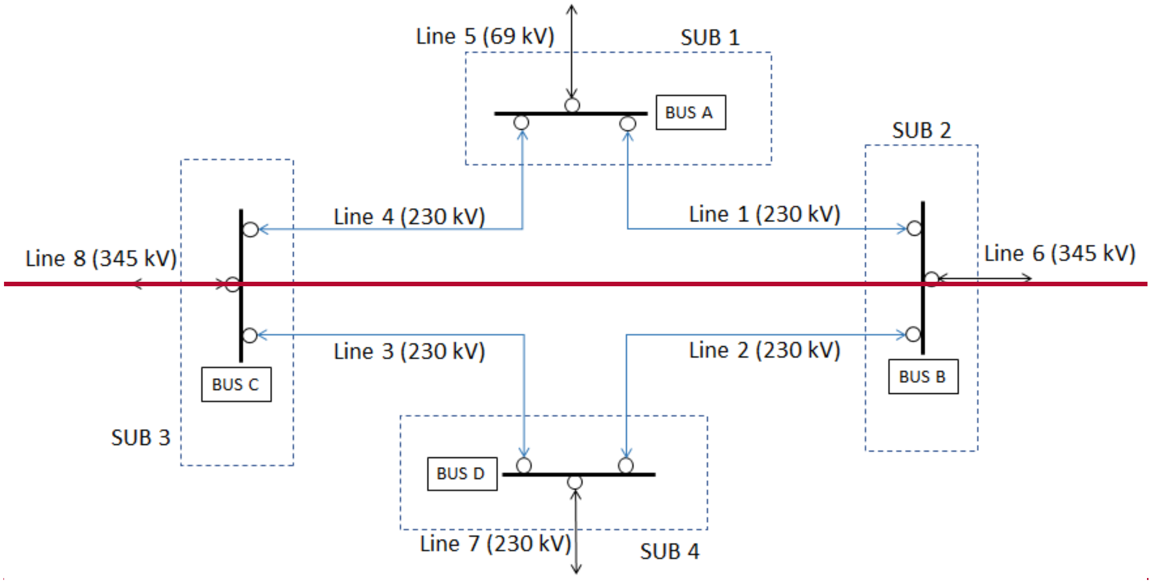
  ~~In the terms of applicable BES Transmission Lines, the following should be considered:~~

  - ~~All BES Transmission Lines that are energized at voltages between 100 kV and 499 kV and are monitored and controlled by a Control Center, including associated data center(s).~~

- ~~All BES Transmission Lines, including those that connect to neighboring entities, that are monitored and controlled by the Responsible Entity's Control Center, including associated data center(s).~~
- ~~Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line. For example, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~
- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. For example, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

~~Criterion 2.12 Examples:~~

~~In example 1 below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.~~



~~Example 1~~

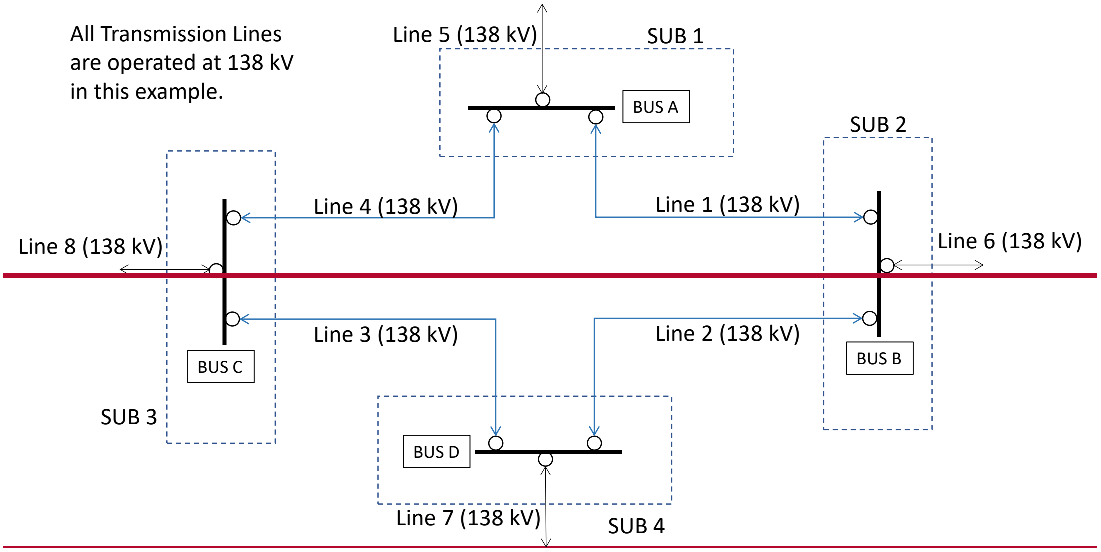
~~The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 6100, which is above the minimum threshold for the medium impact rating required in Criterion 2.12. In accordance with Criterion 2.12, the BES Cyber System(s) associated with the Control Center should be categorized as medium impact BES Cyber System(s).~~

~~Voltage Value of a Line~~	~~Weight Value per Line~~	~~Applicable Lines~~	~~Weighted Value~~
~~less than 100 kV~~ ~~(not applicable)~~	~~(not applicable)~~	~~Line 5~~	~~N/A~~
~~100 kV to 199 kV~~	~~250~~	~~None~~	~~0~~
~~200 kV to 299 kV~~	~~700~~	~~Line 1, Line 2, Line 3, Line 4, Line 7~~	~~3500~~
~~300 kV to 499 kV~~	~~1300~~	~~Line 6, Line 8~~	~~2600~~
~~500 kV and above~~	~~0~~	~~None~~	~~0~~

~~Calculation~~

~~700+700+700+700+700+1300+1300 = 6100~~

~~In the additional example below, BES Cyber System(s) are associated with a Control Center that monitors and controls eight BES Transmission Lines. In order to calculate the Control Center's aggregate weighted value, the Responsible Entity should reference the table located in Criterion 2.12 and sum the weighted values for each BES Transmission Line.~~



~~Example 2~~

~~The weighted value for each BES Transmission Line is detailed in the following table by voltage classification. The calculation of the weighted values is demonstrated below and equates to an aggregate weighted value of 2000, which is below the minimum threshold for a medium impact rating required in Criterion 2.12. The BES Cyber System(s) associated with the Control Center in this example should be categorized as a low impact BES Cyber System(s) pursuant to Criterion 3.1.~~

~~Voltage Value of a Line~~	~~Weight Value per Line~~	~~Applicable Lines~~	~~Weighted Value~~
~~less than 100 kV~~ ~~(not applicable)~~	~~(not applicable)~~	~~None~~	~~N/A~~
~~100 kV to 199 kV~~	~~250~~	~~Line 1, Line 2, Line 3, Line 4, Line 5, Line 6, Line 7, Line 8~~	~~2000~~
~~200 kV to 299 kV~~	~~700~~	~~None~~	~~0~~
~~300 kV to 499 kV~~	~~1300~~	~~None~~	~~0~~
~~500 kV and above~~	~~0~~	~~None~~	~~0~~

~~Calculation~~

~~250+250+250+250+250+250+250+250= 2000~~

- ~~Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Low Impact Rating~~

~~No additional evaluation is necessary for BES Cyber Systems that have already been identified as high or medium impact. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3 default to low impact. Note that low impact BES Cyber Systems do not require discrete identification, only identification of the asset containing the low impact BES Cyber System(s).~~

~~Restoration Facilities~~

- ~~Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.~~

  ~~In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.~~

  ~~The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.~~

  ~~Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.~~

  ~~BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~

  ~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection~~

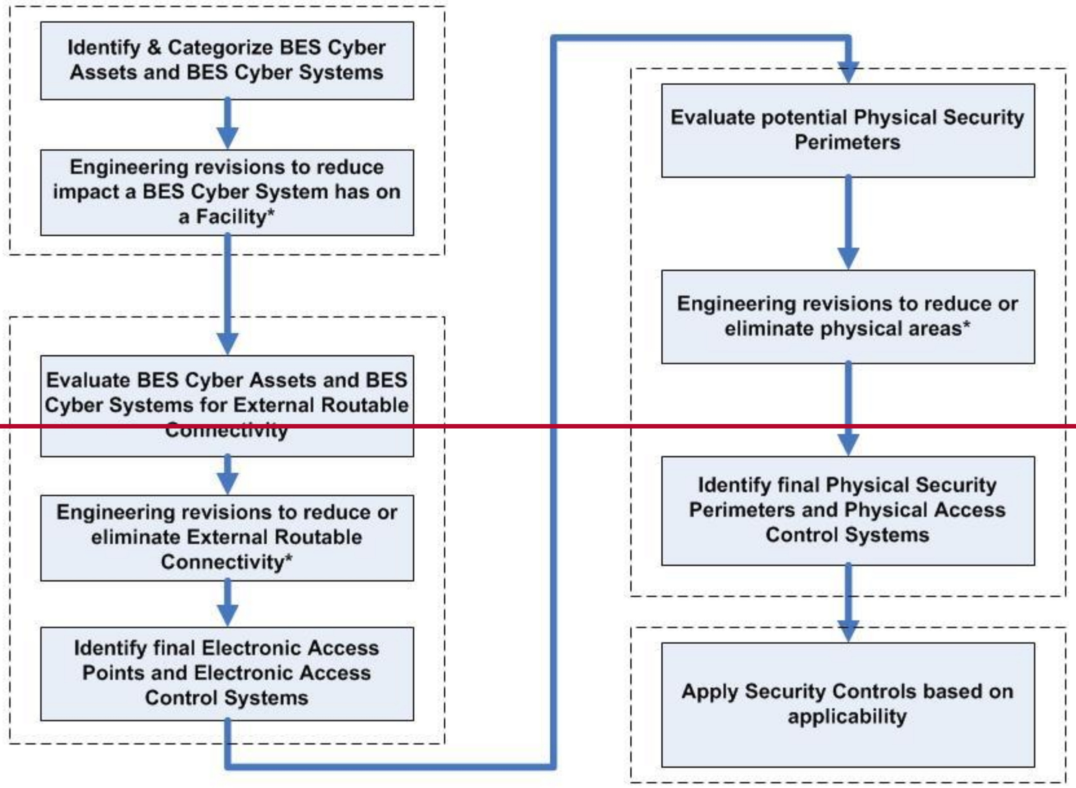
~~point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.~~

~~Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.~~

~~Use Case: CIP Process Flow~~

~~The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.~~

Overview (Generation Facility)



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

~~Rationale~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for R1:~~

~~BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~Rationale for R2:~~

~~The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.~~

~~Appendix 1~~

~~Requirement Number and Text of Requirement~~
~~CIP-002-5.1, Requirement R1~~ ~~R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:~~ ~~i. Control Centers and backup Control Centers;~~ ~~ii. Transmission stations and substations;~~ ~~iii. Generation resources;~~ ~~iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;~~ ~~v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and~~ ~~vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.~~ ~~1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;~~ ~~1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and~~ ~~1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).~~ ~~Attachment 1, Criterion 2.1~~ ~~2. Medium Impact Rating (M)~~ ~~Each BES Cyber System, not included in Section 1 above, associated with any of the following:~~ ~~a. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~

~~Questions~~

~~Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."~~

~~The Interpretation Drafting Team identified the following questions in the RFI:~~

1. ~~Whether the phrase "shared BES Cyber Systems" means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~
2. ~~Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~
3. ~~If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~Responses~~

~~**Question 1: Whether the phrase "shared BES Cyber Systems," means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?**~~

~~The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states "Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…" Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states "*Each BES Cyber System*…associated with any of the following [criteria]." (emphasis added)~~

~~Additionally, the Background section of CIP-002-5.1 states that "[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System." The Background section also provides:~~

> ~~The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~**Question 2: Whether the phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?**~~

~~The phrase "shared BES Cyber Systems" refers to discrete BES Cyber Systems that are shared by multiple generation units.~~

~~The use of the term "shared" is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:~~

> ~~Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1:~~ ~~**Impact Rating of Generation Resource Shared BES Cyber Systems**~~ ~~for further information and examples.~~

~~**Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?**~~

~~The phrase applies to each discrete BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23–April 21, 2016
SAR posted for comment	June 1–June 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21–March 22, 2021
63-day formal comment period with ballot	June 30 –September 1, 2021
53-day formal comment period with ballot	February 18 – April 12, 2022
45-day formal comment period with ballot	August 17 – September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 – 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 CIP Definitions"

A. Introduction

1. **Title:** Cyber Security — BES Cyber System Categorization

2. **Number:** CIP-002-~~5.1a~~7

3. **Purpose:** To identify and categorize BES Cyber Systems (BCS) and their associated BES Cyber Assets (BCA) for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those ~~BES Cyber Systems~~BCS could have on the reliable operation of the ~~BES.~~Bulk Electric System (BES). Identification and categorization of ~~BES Cyber Systems~~BCS support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1. **Balancing Authority**

      4.1.2. **Distribution Provider that owns** one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

            4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and

including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

~~**4.1.5. Interchange Coordinator or Interchange Authority**~~

~~4.1.6.~~4.1.5. **Reliability Coordinator**

~~4.1.7.~~4.1.6. **Transmission Operator**

~~4.1.8.~~4.1.7. **Transmission Owner**

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. ~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme~~Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-~~5.1a~~7:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**5.**~~ **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”

~~1. **24 Months Minimum** – CIP-002-5.1a shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required CIP-002-5.1a shall become effective on the first day of the ninth calendar quarter following Board of Trustees’ approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

~~**6. Background:**~~

~~This standard provides “bright-line” criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.~~

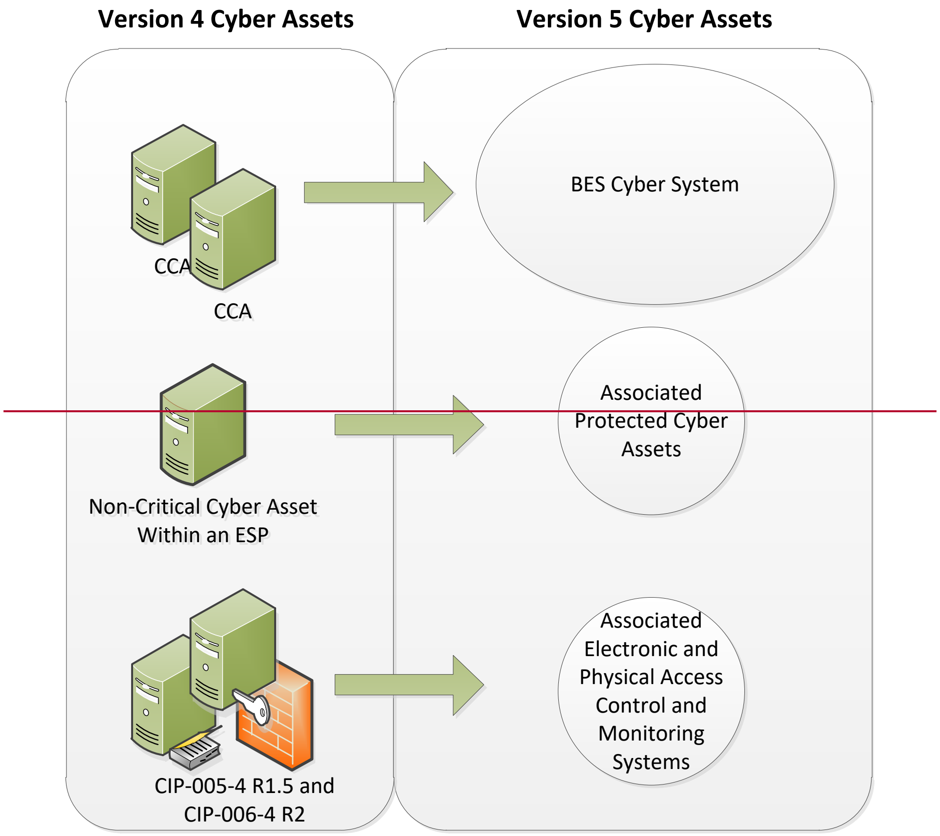
~~Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

5. ~~Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS,~~

~~which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~BES Cyber Systems~~

~~One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.~~



~~In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.~~

~~Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.~~

~~It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Reliable Operation of the BES~~

~~The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.~~

~~Real-time Operations~~

~~One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.~~

~~Categorization Criteria~~

~~The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES~~

~~Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.~~

~~This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.~~

~~Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems~~

~~BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:~~

> **~~Electronic Access Control or Monitoring Systems (“EACMS”)~~** ~~– Examples include: Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.~~
>
> **~~Physical Access Control Systems (“PACS”)~~**~~– Examples include: authentication servers, card systems, and badge control systems.~~
>
> **~~Protected Cyber Assets (“PCA”)~~** ~~– Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.~~

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of ~~parts~~Parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** ~~Special Protection Systems~~RAS that support the reliable operation of the ~~Bulk Electric System~~BES; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact ~~BES Cyber Systems~~BCS according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact ~~BES Cyber Systems~~BCS according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact ~~BES Cyber System~~BCS according to Attachment 1, Section 3, if any (a discrete list of low impact ~~BES Cyber Systems~~BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1~~, and Parts 1.1 and 1.2~~.

R2. ~~The~~Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

~~The Regional Entity shall serve as the~~ "Compliance Enforcement Authority ~~("CEA") unless the applicable~~" means NERC or the Regional Entity, or any entity ~~is owned, operated, or controlled~~as otherwise designated by ~~the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC~~ an Applicable Governmental Authority, in their respective roles of monitoring and/or ~~other applicable governmental authority shall serve as the CEA.~~enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Assessment Processes~~Enforcement Program:

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~
- ~~Complaint~~

~~1.4. Additional Compliance Information~~

- ~~None~~

~~2. Table of Compliance Elements~~

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-002-~~5.1a~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, five percent or fewer of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than five percent but less than or equal to 10 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact ~~BES Cyber Systems~~BCS, more than 10 percent but less than or equal to 15 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 15 percent of identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and

R #	Violation Severity Levels (CIP-002-~~5.1a~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	medium impact ~~BES Cyber Systems~~BCS, five or fewer identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, five percent or fewer high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, five or fewer high or medium ~~BES Cyber Systems~~BCS have not been identified.	incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~and BES Cyber Systems~~BCS, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than five percent but less than or equal to 10 percent high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than five	incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact ~~and BES Cyber Assets~~BCS, more than 10 but less than or equal to 15 identified ~~BES Cyber Assets~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 10 percent but less than or equal to 15 percent high or medium ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact ~~BES Cyber Systems~~BCS, more than 10 but	medium impact ~~BES Cyber Systems~~BCS, more than 15 identified ~~BES Cyber Systems~~BCS have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact ~~BES Cyber Systems~~BCS, more than 15 percent of high or medium impact ~~BES Cyber Systems~~BCS have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact ~~BES Cyber Systems~~BCS have not been identified.

R #	Violation Severity Levels (CIP-002-~~5.1a~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		but less than or equal to 10 high or medium ~~BES Cyber Systems~~BCS have not been identified.	less than or equal to 15 high or medium ~~BES Cyber Systems~~BCS have not been identified.	
R2	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (~~R2~~Part 2.1) OR The Responsible Entity did not complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (~~R2~~Part 2.2)	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (~~R2~~Part2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (~~R2~~Part 2.2)	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (~~R2~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (~~R2~~Part 2.2)	The Responsible Entity did not complete its review and update for the identification required for Requirement R1 within 18 calendar months of the previous review. (~~R2~~Part 2.1) OR The Responsible Entity failed to complete its approval of the identifications required by Requirement R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (~~R2~~Part 2.2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-002-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5.1	9/30/13	Replaced “Devices” with “Systems” in a definition in background section.	Errata
5.1	11/22/13	FERC Order issued approving CIP-002-5.1.	
5.1a	11/02/16	Adopted by the NERC Board of Trustees.	
5.1a	12/14/2016	FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.	
6	5/14/2020	Adopted by the NERC Board of Trustees.	Modified Criterion 2.12.
7	TBD	Virtualization Modifications	

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High ~~Impact Rating (H)~~impact rating**

   Each ~~BES Cyber System~~BCS used by and located at any of the following:

   1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

   1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

   1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

   1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium ~~Impact Rating (M)~~impact rating**

   Each ~~BES Cyber System~~BCS, not included in Section 1 above, associated with any of the following:

   2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

   2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only ~~BES Cyber Systems~~BCS that meet this criterion are ~~those~~each discrete shared ~~BES Cyber Systems~~BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each ~~Special Protection System (SPS), Remedial Action Scheme (~~RAS~~),~~ or automated switching System that operates BES Elements, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in ~~High Impact Rating (H)~~high impact rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in ~~High Impact Rating (H),~~high impact rating, above.

2.13. Each Control Center or backup Control Center, not already included in ~~High Impact Rating (H)~~high impact rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low ~~Impact Rating (L)~~impact rating

~~BES Cyber Systems~~BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. ~~Special Protection Systems~~RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.~~

~~For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.~~

~~CIP-002-5.1a~~

~~CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."~~

~~The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber~~

~~Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:~~

~~Dynamic Response to BES conditions~~
~~Balancing Load and Generation~~
~~Controlling Frequency (Real Power)~~
~~Controlling Voltage (Reactive Power)~~
~~Managing Constraints~~
~~Monitoring & Control~~
~~Restoration of BES~~
~~Situational Awareness~~
~~Inter-Entity Real-Time Coordination and Communication~~

~~Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.~~

~~Entity Registration~~	~~RC~~	~~BA~~	~~TOP~~	~~TO~~	~~DP~~	~~GOP~~	~~GO~~
~~Dynamic Response~~		~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Balancing Load & Generation~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~	~~X~~
~~Controlling Frequency~~		~~X~~				~~X~~	~~X~~
~~Controlling Voltage~~			~~X~~	~~X~~	~~X~~		~~X~~
~~Managing Constraints~~	~~X~~		~~X~~			~~X~~	
~~Monitoring and Control~~			~~X~~			~~X~~	
~~Restoration~~			~~X~~			~~X~~	
~~Situation Awareness~~	~~X~~	~~X~~	~~X~~			~~X~~	
~~Inter-Entity coordination~~	~~X~~	~~X~~	~~X~~	~~X~~		~~X~~	~~X~~

~~Dynamic Response~~

~~The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:~~

- ~~Spinning reserves (contingency reserves)~~
    - ~~Providing actual reserve generation when called upon (GO,GOP)~~
    - ~~Monitoring that reserves are sufficient (BA)~~
- ~~Governor Response~~
    - ~~Control system used to actuate governor response (GO)~~
- ~~Protection Systems (transmission & generation)~~
    - ~~Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)~~
    - ~~Zone protection for breaker failure (DP, TO, TOP)~~
    - ~~Breaker protection (DP, TO, TOP)~~
    - ~~Current, frequency, speed, phase (TO,TOP, GO,GOP)~~
- ~~Special Protection Systems or Remedial Action Schemes~~
    - ~~Sensors, relays, and breakers, possibly software (DP, TO, TOP)~~
- ~~Under and Over Frequency relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Under and Over Voltage relay protection (includes automatic load shedding)~~
    - ~~Sensors, relays & breakers (DP)~~
- ~~Power System Stabilizers (GO)~~

~~Balancing Load and Generation~~

~~The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:~~

- ~~Calculation of Area Control Error (ACE)~~
    - ~~Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)~~
    - ~~Software used to perform calculation (BA)~~
- ~~Demand Response~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP,DP)~~
- ~~Manually Initiated Load shedding~~
    - ~~Ability to identify load change need (BA)~~
    - ~~Ability to implement load changes (TOP, DP)~~

- ~~Non-spinning reserve (contingency reserve)~~
    - ~~Know generation status, capability, ramp rate, start time (GO, BA)~~
    - ~~Start units and provide energy (GOP)~~

~~Controlling Frequency (Real Power)~~

~~The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:~~

- ~~Generation Control (such as AGC)~~
    - ~~ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)~~
    - ~~Software to calculate unit adjustments (BA)~~
    - ~~Transmit adjustments to individual units (GOP)~~
    - ~~Unit controls implementing adjustments (GOP)~~
- ~~Regulation (regulating reserves)~~
    - ~~Frequency source, schedule (BA)~~
    - ~~Governor control system (GO)~~

~~Controlling Voltage (Reactive Power)~~

~~The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:~~

- ~~Automatic Voltage Regulation (AVR)~~
    - ~~Sensors, stator control system, feedback (GO)~~
- ~~Capacitive resources~~
    - ~~Status, control (manual or auto), feedback (TOP, TO,DP)~~
- ~~Inductive resources (transformer tap changer, or inductors)~~
    - ~~Status, control (manual or auto), feedback (TOP,TO,DP)~~
- ~~Static VAR Compensators (SVC)~~
    - ~~Status, computations, control (manual or auto), feedback (TOP, TO,DP)~~

~~Managing Constraints~~

~~Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:~~

- ~~Available Transfer Capability (ATC) (TOP)~~
- ~~Interchange schedules (TOP, RC)~~
- ~~Generation re-dispatch and unit commit (GOP)~~
- ~~Identify and monitor SOL's & IROL's (TOP, RC)~~
- ~~Identify and monitor Flow gates (TOP, RC)~~

~~Monitoring and Control~~

~~Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:~~

- ~~All methods of operating breakers and switches~~
  - ~~SCADA (TOP, GOP)~~
  - ~~Substation automation (TOP)~~

~~Restoration of BES~~

~~The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:~~

- ~~Restoration including planned cranking path~~
  - ~~Through black start units (TOP, GOP)~~
  - ~~Through tie lines (TOP, GOP)~~
- ~~Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)~~
- ~~Coordination (TOP, TO, BA, RC, DP, GO, GOP)~~

~~Situational Awareness~~

~~The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:~~

- ~~Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)~~
- ~~Change management (TOP,GOP,RC,BA)~~
- ~~Current Day and Next Day planning (TOP)~~
- ~~Contingency Analysis (RC)~~
- ~~Frequency monitoring (BA, RC)~~

~~Inter-Entity Coordination~~

~~The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:~~

- ~~Scheduled interchange (BA,TOP,GOP,RC)~~
- ~~Facility operational data and status (TO, TOP, GO, GOP, RC, BA)~~
- ~~Operational directives (TOP, RC, BA)~~

~~Applicability to Distribution Providers~~

~~It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.~~

~~Requirement R1:~~

~~Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.~~

~~Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.~~

~~**Attachment 1**~~

~~**Overall Application**~~

~~In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.~~

- ~~When the drafting team uses the term “Facilities”, there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.~~
- ~~In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.~~
- ~~It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.~~

~~**High Impact Rating (H)**~~

~~This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some~~

~~of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.~~

~~The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.~~

~~Additional thresholds as specified in the criteria apply for this category.~~

~~Medium Impact Rating (M)~~

~~Generation~~

~~The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.~~

- ~~Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.~~

  ~~In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.~~

  ~~By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.~~

~~The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.~~

- ~~In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.~~

  ~~If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.~~

  ~~The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.~~

- ~~Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~

  ~~IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.~~

- ~~Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.~~

- ~~Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.~~

- ~~Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Transmission~~

~~The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.~~

- ~~Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.~~

- ~~Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.~~

~~It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.~~

- ~~Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:~~

  - ~~Excluded radial facilities that would only provide support for single generation facilities.~~

  - ~~Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.~~

~~The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.~~

~~Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:~~

  - ~~230 kV –> 700 MVA~~

  - ~~345 kV –> 1,300 MVA~~

  - ~~500 kV –> 2,000 MVA~~

  - ~~765 kV –> 3,000 MVA~~

~~In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:~~

  - ~~For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate~~

~~connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.~~

- ~~Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.~~

- ~~Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.~~

~~Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.~~

1. ~~The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.~~
2. ~~The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.~~

~~The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.~~

- ~~Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2,~~ ~~**Establish and Communicate System Operating Limits**~~~~, R5.1.1 and R5.1.3.~~

- ~~Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.~~

- ~~Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.~~

- ~~Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.~~

- ~~Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.~~

  ~~This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

~~In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.~~

~~The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.~~

- ~~Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.~~

- ~~Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.~~

~~Low Impact Rating (L)~~

~~BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.~~

~~Restoration Facilities~~

- ~~Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.~~

  ~~In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.~~

  ~~The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.~~

~~Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.~~

~~BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.~~

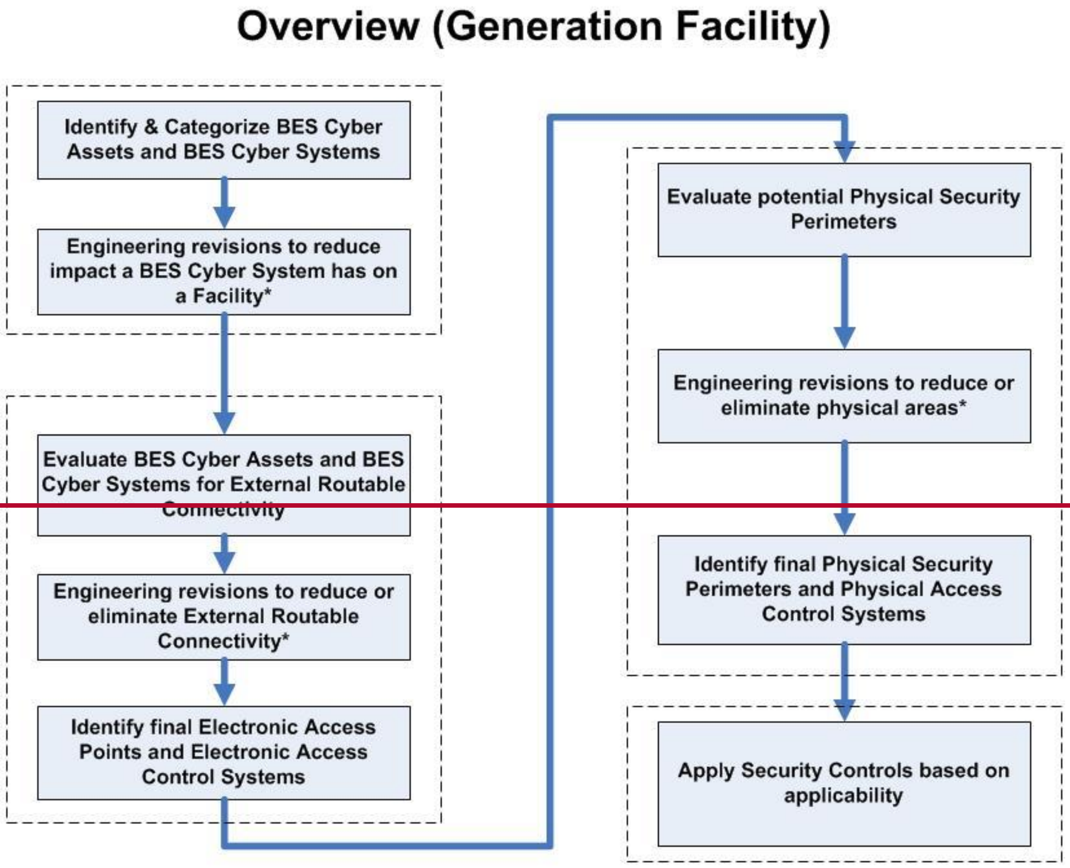
~~Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."~~

- ~~BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.~~

~~Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.~~

~~Use Case: CIP Process Flow~~

~~The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.~~



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for R1:~~

~~BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.~~

~~Rationale for R2:~~

~~The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.~~

~~Version~~	~~Date~~	~~Action~~	~~Change Tracking~~
~~1~~	~~1/16/06~~	~~R3.2 — Change "Control Center" to "control center."~~	~~3/24/06~~
~~2~~	~~9/30/09~~	~~Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.~~ ~~Removal of reasonable business judgment.~~ ~~Replaced the RRO with the RE as a Responsible Entity.~~ ~~Rewording of Effective Date.~~ ~~Changed compliance monitor to Compliance Enforcement Authority.~~	
~~3~~	~~12/16/09~~	~~Updated version number from -2 to -3.~~ ~~Approved by the NERC Board of Trustees.~~	~~Update~~

~~3~~	~~3/31/10~~	~~Approved by FERC.~~	
~~4~~	~~12/30/10~~	~~Modified to add specific criteria for Critical Asset identification.~~	~~Update~~
~~4~~	~~1/24/11~~	~~Approved by the NERC Board of Trustees.~~	~~Update~~
~~5~~	~~11/26/12~~	~~Adopted by the NERC Board of Trustees.~~	~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.~~
~~5.1~~	~~9/30/13~~	~~Replaced "Devices" with "Systems" in a definition in background section.~~	~~Errata~~
~~5.1~~	~~11/22/13~~	~~FERC Order issued approving CIP-002-5.1.~~	
~~5.1a~~	~~11/02/16~~	~~Adopted by the NERC Board of Trustees.~~	
~~5.1a~~	~~12/14/2016~~	~~FERC letter Order approving CIP-002-5.1a. Docket No. RD17-2-000.~~	

~~Appendix 1~~

~~**Requirement Number and Text of Requirement**~~
~~CIP-002-5.1, Requirement R1~~ ~~R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:~~ ~~i. Control Centers and backup Control Centers;~~ ~~ii. Transmission stations and substations;~~ ~~iii. Generation resources;~~ ~~iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;~~ ~~v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and~~ ~~vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.~~ ~~1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;~~ ~~1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and~~ ~~1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).~~ ~~Attachment 1, Criterion 2.1~~ ~~2. Medium Impact Rating (M)~~ ~~Each BES Cyber System, not included in Section 1 above, associated with any of the following:~~ ~~2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.~~
~~**Questions**~~
~~Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase "shared BES Cyber Systems."~~ ~~The Interpretation Drafting Team identified the following questions in the RFI:~~

1. ~~Whether the phrase “shared BES Cyber Systems” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~
2. ~~Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~
3. ~~If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~Responses~~

~~Question 1: Whether the phrase “shared BES Cyber Systems,” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?~~

~~The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states “Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…” Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states “*Each BES Cyber System*…associated with any of the following [criteria].” (emphasis added)~~

~~Additionally, the Background section of CIP-002-5.1 states that “[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System.” The Background section also provides:~~

> ~~The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.~~

~~Question 2: Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?~~

~~The phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple generation units.~~

~~The use of the term “shared” is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:~~

> ~~Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating~~

~~criteria 2.1 and 2.2. For criterion 2.1 "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection." For criterion 2.2: "BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1:~~ **~~Impact Rating of Generation Resource Shared BES Cyber Systems~~** ~~for further information and examples.~~

~~Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?~~

~~The phrase applies to each discrete BES Cyber System.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29, 2023

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 CIP Definitions”.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-10

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-003-10:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. **Effective Dates:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1.** For its high impact and medium impact BCS, if any:
  - **1.1.1.** Personnel and training (CIP-004);
  - **1.1.2.** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
  - **1.1.3.** Physical security of BCS (CIP-006);
  - **1.1.4.** System security management (CIP-007);
  - **1.1.5.** Incident reporting and response planning (CIP-008);
  - **1.1.6.** Recovery plans for BCS (CIP-009);
  - **1.1.7.** Configuration change management and vulnerability assessments (CIP-010);
  - **1.1.8.** Information protection (CIP-011); and
  - **1.1.9.** Declaring and responding to CIP Exceptional Circumstances.
- **1.2.** For its assets identified in CIP-002 containing low impact BCS, if any:
  - **1.2.1.** Cyber security awareness;
  - **1.2.2.** Physical security controls;
  - **1.2.3.** Electronic access controls;
  - **1.2.4.** Cyber Security Incident response;
  - **1.2.5.** Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation;
  - **1.2.6.** Vendor electronic remote access security controls; and
  - **1.2.7.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that

include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with mandatory and enforceable Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not address one of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager	The Responsible Entity did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did	The Responsible Entity did not address three of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did	The Responsible Entity did not address four or more of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BCS as required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address one of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar	complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address two of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (Part 1.2) OR	complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS, but did not address three of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part 1.2) OR	impact BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part 1.1) OR The Responsible Entity did not address four or more of the seven topics required by Requirement R1. (Part 1.2) OR The Responsible Entity did not have any documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1. (R1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	months of the previous review. (Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part 1.2)	The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part 1.2)	within 18 calendar months of the previous approval. (R1.2)
R2	The Responsible Entity failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document its cyber security plan(s) for	The Responsible Entity failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity failed to document physical security	The Responsible Entity failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to permit only necessary inbound and outbound electronic access controls	The Responsible Entity failed to document and implement one or more cyber security plan(s) according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2)	controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity failed to implement authentication for all Dial-up Connectivity according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to document the	according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR The Responsible Entity documented failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2,	

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-003-10)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>OR
The Responsible Entity failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)
OR
The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)</td><td>determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2)
OR
The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2)
OR
The Responsible Entity failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment</td><td>Attachment 1, Section 5.1. (Requirement R2)
OR
The Responsible Entity failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2)
OR
The Responsible Entity failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2)
OR
The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote</td><td></td></tr>
</table>

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		1, Section 5.2. (Requirement R2) OR The Responsible Entity failed to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)	access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	
R3	The Responsible Entity did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days	The Responsible Entity did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity did not identify, by name, a CIP Senior Manager. OR The Responsible Entity did not document changes to the CIP Senior Manager within 60

R #	Violation Severity Levels (CIP-003-10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	of the change. (Requirement R3)			calendar days of the change. (Requirement R3)
R4	The Responsible Entity did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-003-10 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026
10	TBD	Virtualization Modifications	

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. <u>TCA and Removable Media Malicious Code Risk Mitigation</u>: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS, through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
    a. The asset, if any, or the locations of the low impact BCS within the asset; and
    b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).
2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process

documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. <u>TCA and Removable Media Malicious Code Risk Mitigation</u>:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - security information management logging alerts;
    - time-of-need session initiation;
    - session recording;
    - system logs; or
    - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
    - disabling vendor electronic remote access user or system accounts;
    - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
    - disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;

  - Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
  - administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
  - other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
   - Anti-malware technologies;
   - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
   - Automated or manual log reviews;
   - alerting; or
   - other operational, procedural, or technical controls.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29, 2023

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 CIP Definitions”.

A. Introduction

1. **Title:** Cyber Security — Security Management Controls

2. **Number:** CIP-003-10~~9~~

3. **Purpose:** To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

3. **Applicability:**

   3.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   3.1.1. **Balancing Authority**

   3.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   3.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   3.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   3.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   3.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   3.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   3.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   3.1.3. **Generator Operator**

   3.1.4. **Generator Owner**

   3.1.5. **Reliability Coordinator**

3.1.6. Transmission Operator

3.1.7. Transmission Owner

3.2. ~~1.1.~~ **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

3.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

3.2.1.1. Each UFLS or UVLS System that:

3.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

3.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

3.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

3.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

3.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

3.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

3.2.3. Exemptions: The following are exempt from Standard CIP-003-10:

3.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

3.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (~~ESPs~~ESP).

3.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**3.2.3.3.**~~**3.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**3.2.3.4.**~~**3.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan~~ for CIP-003-9.~~."

B. Requirements and Measures

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. For its high impact and medium impact ~~BES Cyber Systems~~BCS, if any:

1.1.1. Personnel and training (CIP~~-~~-004);

1.1.2. Electronic Security Perimeters (CIP~~-~~-005) including Interactive Remote Access;

1.1.3. Physical security of ~~BES Cyber Systems~~BCS (CIP~~-~~-006);

1.1.4. System security management (CIP~~-~~-007);

1.1.5. Incident reporting and response planning (CIP~~-~~-008);

1.1.6. Recovery plans for ~~BES Cyber Systems~~BCS (CIP~~-~~-009);

1.1.7. Configuration change management and vulnerability assessments (CIP~~-~~-010);

1.1.8. Information protection (CIP~~-~~-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2. For its assets identified in CIP~~-~~-002 containing low impact ~~BES Cyber Systems~~BCS, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls;

1.2.4. Cyber Security Incident response;

1.2.5. Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation;

1.2.6. Vendor electronic remote access security controls; and

1.2.7. Declaring and responding to CIP Exceptional Circumstances.

M1.~~-~~ Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity with at least one asset identified in CIP~~-~~-002 containing low impact ~~BES Cyber Systems~~BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]* ~~*[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*~~

Note: An inventory, list, or discrete identification of low impact ~~BES Cyber Systems~~BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2.~~-~~_Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3.~~-~~_An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4.~~-~~_An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with ~~the NERC~~mandatory and enforceable Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non~~-~~-compliant, it shall keep information related to the non~~-~~-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records~~,~~ and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address one of the nine topics required by Requirement R1. (~~R1~~Part1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part~~R~~1.1)	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address two of the nine topics required by Requirement R1. (Part 1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R1~~Part1.1) OR The Responsible Entity did not complete its approval of the one or more documented	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address three of the nine topics required by Requirement R1. (Part ~~R~~1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (~~R1~~Part 1.1) OR The Responsible Entity did not complete its approval of the one or more documented	The Responsible Entity ~~documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but~~ did not address four or more of the nine topics required by Requirement R1. (Part~~R~~1.1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1. (Part~~R~~1.1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by Requirement R1 within 18 calendar months of the

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (Part~~R~~1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact BCS~~BES Cyber Systems~~, but did not address one of the seven topics required by Requirement R1. (Part~~R~~1.2) OR	cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part~~R~~1.1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address two of the seven topics required by Requirement R1. (Part~~R~~1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 within 16	cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Requirement R1) OR The Responsible Entity documented one or more cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS, but did not address three of the seven topics required by Requirement R1. (Part~~R~~1.2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required	previous review. (Requirement R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact ~~BES Cyber Systems~~BCS as required by ~~R1~~Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part~~R~~1.1) OR The Responsible Entity ~~documented one or more cyber security policies for its assets identified in CIP-002 containing low impact~~ ~~BES Cyber Systems, but~~ did not address four or more of the seven topics required by Requirement R1. (Part~~R~~1.2) OR The Responsible Entity did not have any documented cyber

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	The Responsible Entity did not complete its review of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (Part~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact BCS ~~BES Cyber Systems~~ as required by Requirement R1 by the CIP Senior Manager within 15 calendar months but did complete this approval in less than or	calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (~~R1~~Part 1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (Part ~~R~~1.2)	by Requirement R1 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (Part~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (Part~~R~~1.2)	security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~ BCS as required by Requirement R1. (Part~~R~~1.2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its assets identified in CIP-002 containing low impact ~~BES Cyber Systems~~BCS as required by Requirement R1 by the CIP Senior Manager within 18 calendar months of the previous approval. (Part~~R~~1.2)

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	equal to 16 calendar months of the previous approval. (~~R1~~Part 1.2)			
R2	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document cyber security awareness according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~implemented electronic access controls but~~ failed to document its cyber security plan(s) for electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber~~	The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to reinforce cyber security practices at least once every 15 calendar months according to Requirement R2, Attachment 1, Section 1. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber~~	The Responsible Entity ~~documented the physical access controls for its assets containing low impact BES Cyber Systems, but~~ failed to implement the physical security controls according to Requirement R2, Attachment 1, Section 2. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls for its assets containing low impact BES Cyber Systems, but~~ failed to permit only necessary inbound and outbound electronic access controls according to Requirement R2, Attachment 1, Section 3.1. (Requirement R2) OR	The Responsible Entity failed to document and implement one or more cyber security plan(s) ~~for its assets containing low impact BES Cyber Systems~~ according to Requirement R2, Attachment 1. (Requirement R2)

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document one or more Cyber Security Incident response plan(s) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to update each Cyber Security Incident response plan(s) within 180 days according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for~~	~~security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document electronic access controls according to Requirement R2, Attachment 1, Section 3. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for electronic access controls but~~ failed to implement authentication for all Dial-up Connectivity ~~that provides access to low impact BES Cyber System(s), per Cyber Asset capability~~ according to Requirement R2, Attachment 1, Section 3.2 (Requirement R2) OR The Responsible Entity ~~documented one or more incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES~~	The Responsible Entity ~~documented one or more Cyber Security Incident response plan(s) within its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to test each Cyber Security Incident response plan(s) at least once every 36 calendar months according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident, but~~ failed to notify the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR	

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Transient Cyber Assets and Removable Media, but~~ failed to manage its Transient Cyber Asset(s) according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets, but~~ failed to document the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity implemented vendor electronic remote access security controls but failed to document its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	~~Cyber Systems, but~~ failed to include the process for identification, classification, and response to Cyber Security Incidents according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its cyber security plan(s) for its assets containing low impact BES Cyber Systems, but~~ failed to document the determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC) according to Requirement R2, Attachment 1, Section 4. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and~~	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for Transient Cyber Asset managed by the Responsible Entity according to Requirement R2, Attachment 1, Section 5.1. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR	

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		~~Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Asset managed by the Responsible Entity according to Requirement R2, Attachment 1, Sections 5.1 and 5.3. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to document mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Requirement R2, Attachment 1, Section 5.2. (Requirement R2) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but~~ failed to implement mitigation for the threat of detected malicious code on the Removable Media prior to connecting Removable Media according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity failed to document and implement its cyber security process for vendor electronic remote access security controls according to Requirement R2, Attachment 1, Section 6. (Requirement R2)	

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		to implement the Removable Media section(s) according to Requirement R2, Attachment 1, Section 5.3. (Requirement R2) OR The Responsible Entity documented its cyber security process for vendor electronic remote access security controls, but failed to implement vendor electronic remote access security controls according to Requirement R2. Attachment 1, Section 6. (Requirement R2)		
R3	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R3)	The Responsible Entity ~~has~~ did not identify~~ied~~, by name, a CIP Senior Manager. OR The Responsible Entity ~~has identified by name a CIP Senior Manager, but~~ did not document changes to the CIP Senior Manager within 60 calendar days of the change. (Requirement R3)

R #	Violation Severity Levels (CIP-003-~~9~~10)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 30 calendar days but did document this change in less than 40 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (Requirement R4)	The Responsible Entity ~~has used delegated authority for actions where allowed by the CIP Standards, but~~ does not have a process to delegate actions from the CIP Senior Manager. (Requirement R4) OR The Responsible Entity ~~has identified a delegate by name, title, date of delegation, and specific actions delegated, but~~ did not document changes to the delegate within 60 calendar days of the change. (Requirement R4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-003-10 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-003-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.

Version	Date	Action	Change Tracking
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC Order issued approving CIP-003-6. Docket No. RM15-14-000	
7	2/9/17	Adopted by the NERC Board of Trustees.	Revised to address FERC Order No. 822 directives regarding (1) the definition of LERC and (2) transient devices.
7	4/19/18	FERC Order issued approving CIP-003-7. Docket No. RM17-11-000	
8	5/9/19	Adopted by the NERC Board of Trustees.	Removed SPS references. Revised to address FERC Order No. 843 regarding mitigating the risk of malicious code.
8	7/31/2019	FERC Order issued approving CIP-003-8. Docket No. RD19-5-000.	
9	11/16/2022	Adopted by the NERC Board of Trustees.	Revisions to address NERC Board Resolution and the Supply Chain Report
9	3/16/2023	FERC Order issued approving CIP-003-9. Docket No. RD23-3-000.	
9	3/22/2023	Effective Date	April 1, 2026

10	TBD	Modified by Project 2016-02	

Attachment 1

Required Sections for Cyber Security Plan(s)~~ for Assets Containing Low Impact BES Cyber Systems~~

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple~~-~~-impact ~~BES Cyber Systems~~BCS ratings can utilize policies, procedures, and processes for their high or medium impact ~~BES Cyber Systems~~BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. ~~**Section 1.**~~ Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. ~~**Section 2.**~~ Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset, and (2) the Cyber Asset(s~~),~~) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. ~~**Section 3.**~~ Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP~~-~~-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. ~~between~~Between:

- a low impact ~~BES Cyber System(s)~~ BCS; or
- An SCI that supports a low impact BCS

and a Cyber ~~Asset~~System(s) outside the asset containing~~ low impact BES Cyber System(s);~~:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

~~i.~~ii. using a routable protocol when entering or leaving the asset containing the low impact ~~BES Cyber System(s);~~BCS or SCI that supports a low impact BCS; and

~~ii.~~iii. not used for time~~-~~-sensitive ~~protection or control functions between intelligent electronic devices (e.g.,~~ communications ~~using protocol IEC TR-61850-90-5 R-GOOSE).~~of Protection Systems.

3.2 Authenticate all Dial~~-~~-up Connectivity, if any, that provides access to low impact ~~BES Cyber System(s),~~BCS or SCI that supports a low impact BCS, per ~~Cyber Asset~~system capability.

Section 4. ~~**Section 4.**~~ Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E~~-~~-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. ~~Transient Cyber Asset~~ TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact ~~BES Cyber Systems~~BCS, through the use of ~~Transient Cyber Assets~~TCA or Removable Media. The plan(s) shall include:

5.1 For ~~Transient Cyber Asset(s)~~TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on~~-~~-demand manner (per ~~Transient Cyber Asset~~TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting ~~the Transient Cyber Asset to a low impact BES Cyber System (per Transient Cyber Asset~~(per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- ~~Other~~Review of other method(s) to mitigate the risk of introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset.~~TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a ~~BES Cyber System~~BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact ~~BES Cyber System~~BCS or SCI that supports a low impact BCS.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access; and

~~**6.1**~~ **6.3** One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s) ~~for Assets Containing Low Impact BES Cyber Systems~~

Section 1. ~~Section 1.~~ Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e~~-~~-mails, memos, or computer~~-~~-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. ~~Section 2.~~ Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:
  a. The asset, if any, or the locations of the low impact ~~BES Cyber Systems~~BCS within the asset; and
  b. The Cyber ~~Asset~~System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. ~~Section 3.~~ Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets~~ containing low impact BES Cyber Systems, ~~, the routable protocol communication ~~between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset~~as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that ~~communication is~~communications are used for time~~-~~-sensitive ~~protection or control functions between intelligent electronic devices~~communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) ~~between the low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s)~~ or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial~~-~~-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial~~-~~-back modems, modems that must be remotely controlled by the control center or control room, or access control on the ~~BES Cyber System~~BCS).

Section 4. ~~Section 4.~~ Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E~~-~~-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. ~~Section 5.~~ ~~Transient Cyber Asset~~TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

~~1.~~ Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of ~~live operating systems or~~ system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that

2. identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset(s)~~TCA managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

   Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on~~-~~-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code~~.~~

Section 6. Vendor Electronic Remote Access Security Controls**:** Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
   - steps to preauthorize access;
   - alerts generated by vendor log on;
   - session monitoring;
   - security information management logging alerts;
   - time-of-need session initiation;
   - session recording;
   - system logs; or
   - other operational, procedural, or technical controls.
2. For Section 6.2, documentation showing:
   - disabling vendor electronic remote access user or system accounts;

- disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
- disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
- Removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
- administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
- other operational, procedural, or technical controls.

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - Automated or manual log reviews;
    - alerting; or
    - other operational, procedural, or technical controls.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29 2023

Anticipated Actions	Date
Final Ballot	April 3 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 CIP Definitions”.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-8

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.

4. **Applicability:**

   4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1. **Balancing Authority**

      4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

            4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

      4.1.3. **Generator Operator**

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. “Applicable Systems”: Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. Effective Dates: See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part.	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS with IRA SCI supporting an Applicable System in this Part	months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity’s criteria or process to evaluate criminal history records checks.
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity’s criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS with IRA SCI supporting an Applicable System in this Part		
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP) (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access (except for medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts; and authorized unescorted physical access (except for medium impact BCS without ERC) that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Examples of evidence may include, but are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	Examples of evidence may include, but are not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual’s ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	authorized unescorted physical access. (Part 2.2) OR The Responsible Entity did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for two individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1)	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2) OR The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)
R5	The Responsible Entity did not revoke individual’s user accounts upon termination action within 30 calendar days of the date of	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal	The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	termination action for one or more individuals. (Part 5.3) OR The Responsible Entity did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	within 24 hours of the termination action for one individual. (Part 5.1) OR The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	complete the removal within 24 hours of the termination action for two individuals. (Part 5.1) OR The Responsible Entity for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action for three or more individuals. (Part 5.1) OR The Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (Requirement R6) OR The Responsible Entity, for four or more individuals, did not authorize provisioned electronic access to

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	The Responsible Entity did not perform the verification required by Part 6.2 within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for one individual, did not remove the individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for two individuals, did remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for three individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for four or more individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-004-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
8	TBD	Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29 2023

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 ~~Draft 5~~CIP Definitions".

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-8

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting BCS.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

      4.1.1. Balancing Authority

      4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

         4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

            4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

            4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

         4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

         4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

      4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R1 – Security Awareness Program			
Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part.	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months ~~(except for medium impact BCS without ERC).~~.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-8 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS with IRA SCI supporting an Applicable System in this Part	months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS with IRA SCI supporting an Applicable System in this Part		
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP) (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
			verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access (except for ~~Medium~~medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts; and authorized unescorted physical access (except for ~~Medium~~medium impact BCS without ERC) that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Examples of evidence may include, but are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	Examples of evidence may include, but are not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: - List of authorized individuals; - List of individuals who have been provisioned access; - Verification that provisioned access is appropriate based on need; and - Documented reconciliation actions, if any.
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a ~~Medium~~medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	authorized unescorted physical access. (Part 2.2) OR The Responsible Entity did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for one individual. (Requirement R3) OR The Responsible Entity did not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for two individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for two individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for three individuals. (Parts 3.2 & 3.4) OR	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR The Responsible Entity did not conduct the personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	The Responsible Entity did not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)	The Responsible Entity did not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity did not include the required checks described in 3.2.1 through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 through 3.4) OR The Responsible Entity did not conduct personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous personnel risk assessments completion date. (Part 3.5)
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1)	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-004-8)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2)
OR
The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for 5% or less of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)</td><td>OR
The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. (Part 4.2)
OR
The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 5% but less than (or equal to) 10% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)</td><td>OR
The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2)
OR
The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 10% but less than (or equal to) 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)</td><td>The Responsible Entity did not authorize electronic access or unescorted physical access based on need for three or more individuals. (Part 4.1)
OR
The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. (Part 4.2)
OR
The Responsible Entity did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification for more than 15% of its BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)</td></tr>
<tr><td>R5</td><td>The Responsible Entity did not revoke individual’s user accounts upon termination action within 30 calendar days of the date of</td><td>The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or complete the removal</td><td>The Responsible Entity did not initiate removal of the ability for unescorted physical access and IRA upon a termination action or</td><td>The Responsible Entity has not implemented any documented program(s) for access revocation for</td></tr>
</table>

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-004-8)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td>termination action for one or more individuals. (Part 5.3)
OR
The Responsible Entity did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4)
OR
The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)</td><td>within 24 hours of the termination action for one individual. (Part 5.1)
OR
The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)</td><td>complete the removal within 24 hours of the termination action for two individuals. (Part 5.1)
OR
The Responsible Entity for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)</td><td>electronic access or unescorted physical access. (Requirement R5)
OR
The Responsible Entity did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action for three or more individuals. (Part 5.1)
OR
The Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)</td></tr>
<tr><td>R6</td><td>The Responsible Entity, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1)
OR</td><td>The Responsible Entity, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1)
OR</td><td>The Responsible Entity, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1)
OR</td><td>The Responsible Entity did not implement one or more documented access management program(s) for BCSI. (Requirement R6)
OR
The Responsible Entity, for four or more individuals, did not authorize provisioned electronic access to</td></tr>
</table>

R #	Violation Severity Levels (CIP-004-8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did not perform the verification required by Part 6.2 within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for one individual, did not remove the individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for two individuals, did remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	The Responsible Entity did not perform the verification required by Part 6.2 within 17 calendar months but less than or equal to 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for three individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.	electronic BCSI or provisioned physical access to physical BCSI. (Part 6.1) OR The Responsible Entity did not perform the verification required by Part 6.2 more than 18 calendar months of the previous verification. (Part 6.2) OR The Responsible Entity, for four or more individuals, did not remove each individual's ability to use provisioned access to BCSI by the timeframe required in Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-004-8 Technical Rationale

~~None.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
8	TBD	~~Modified by Project 2016-02.~~Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29 2023

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 ~~Draft 5~~CIP Definitions".

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-~~7~~8

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems (BCS) by requiring an appropriate level of personnel risk assessment, training, security awareness, and access management in support of protecting ~~BES Cyber Systems~~BCS.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-~~7~~8:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3.**~~**4.2.3.4.** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4.**~~**4.2.3.5.** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.5.**~~**4.2.3.6.** Responsible Entities that identify that they have no ~~BES Cyber Systems~~BCS categorized as high impact or medium impact according to the CIP-002~~-5.1a~~ identification and categorization processes.

~~**5. Effective Dates:** See Implementation Plan for CIP-004-7.~~

~~**6. Background:** Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards~~

~~include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~” Columns in Tables:~~

~~6.1.~~4.3. ”: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies. ~~The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.~~

- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~7~~8 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES~~impact BCS Medium impact BCS Shared Cyber ~~Systems~~Infrastructure (SCI) supporting an Applicable System in this Part. ~~Medium Impact BES Cyber Systems~~	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to ~~BES Cyber~~Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. ~~-~~Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-~~7~~8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-~~7~~8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~7~~8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS~~;~~); and ~~2. PACS~~ 2. Physical Access Control Systems (PACS) Medium ~~Impact BES Cyber Systems~~ impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for ~~BES Cyber Systems~~BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a ~~BES Cyber System's~~BCS electronic interconnectivity and interoperability with other Cyber ~~Assets~~Systems, including Transient Cyber Assets~~,~~ (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

CIP-004-~~7~~8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to ~~applicable Cyber Assets~~Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

CIP-004-~~7~~8 Table R2 – Cyber Security Training Program

Part	Applicable Systems	Requirements	Measures
	Part		

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to ~~BES Cyber~~Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-~~7~~8 Table R3 – ~~-~~Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.
3.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber~~	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
	~~Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	
3.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.
3.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of the Responsible Entity's

CIP-004-~~7~~8 Table R3 – Personnel Risk Assessment Program

Part	Applicable Systems	Requirements	Measures
	2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	conducted according to Parts 3.1 through 3.3.	criteria or process for verifying contractors or service vendors personnel risk assessments.
3.5	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 ~~to~~through 3.4 within the last seven years.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

CIP-004-~~7~~8 Table R4 – Access Management Program

Part	Applicable Systems	Requirements	Measures
4.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; and 4.1.2. Unescorted physical access into a Physical Security Perimeter (PSP) (except for medium impact BCS without ERC).	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a ~~Physical Security Perimeter.~~PSP.
4.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated:	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or

CIP-004-~~7~~8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part		• Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).
4.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~7~~8 Table R5 – Access Revocation

Part	Applicable Systems	Requirements	Measures
5.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access (except for medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.
5.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated:	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts; and authorized unescorted physical access (except for medium impact BCS without ERC) that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible

CIP-004-~~7~~8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part		Entity determines is not necessary.
5.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.
5.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the ~~“~~Applicable Systems~~”~~ identified in *CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1~~.)~~) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI~~.~~ (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.

CIP-004-~~7~~8 Table R6 – Access Management for BES Cyber System Information

Part	Applicable Systems	Requirements	Measures
6.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of dated evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

C. ~~C.~~ Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance.~~-~~ For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- The applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (Part 1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (Part 1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (Requirement R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (Part 1.1)
R2	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train two individuals (with the exception of CIP Exceptional Circumstances) prior to their	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9. (Part 2.1) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train three individuals (with the exception of CIP Exceptional Circumstances) prior to their	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (Requirement R2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9. ~~(~~(Part 2.1) OR

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	being granted authorized electronic and authorized unescorted physical access. (Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train three individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)	The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access. ~~(~~(Part 2.2) OR The Responsible Entity ~~implemented a cyber security training program but failed to~~did not train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date. (Part 2.3)
R3	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting authorized electronic or authorized unescorted	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting authorized electronic or	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing ~~Personnel Risk Assessments (PRAs),~~personnel risk assessments, for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (Requirement R3) OR

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	access for one individual. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for one individual. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~through 3.2.2 for one individual. (Parts 3.2 & 3.4) OR	physical access for two individuals. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for two individuals. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~through 3.2.2 for two individuals. (Parts 3.2 & 3.4)	authorized unescorted physical access for three individuals. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for three individuals. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did not include the required checks described in 3.2.1 ~~and~~through 3.2.2 for	The Responsible Entity ~~has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but~~ did not conduct the ~~PRA~~personnel risk assessments as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals. (Requirement R3) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not confirm identity for four or more individuals. (Parts 3.1 & 3.4) OR The Responsible Entity ~~has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~ did

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not evaluate criminal history records check for access authorization for one individual. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)	OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not evaluate criminal history records check for access authorization for two individuals. (Parts 3.3 & 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)	three individuals. (Parts 3.2 & 3.4) OR The Responsible Entity did ~~conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did~~ not evaluate criminal history records check for access authorization for three individuals. (Parts 3.3 ~~&~~through 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)	not include the required checks described in 3.2.1 ~~and~~through 3.2.2 for four or more individuals. (Parts 3.2 & 3.4) OR ~~The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but~~The Responsible Entity did not evaluate criminal history records check for access authorization for four or more individuals. (Parts 3.3 ~~&~~through 3.4) OR The Responsible Entity did not conduct ~~Personnel Risk Assessments (PRAs)~~personnel risk assessments for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous ~~PRA~~personnel risk assessments completion date. (Part 3.5)

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for 5% or less of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for one individual. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 20 calendar days after the start of a subsequent calendar quarter. ~~(~~(Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 5% but less than (or equal to) 10% of its ~~BES Cyber~~	The Responsible Entity did not authorize electronic access or unescorted physical access based on need for two individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 20 and 30 calendar days after the start of a subsequent calendar quarter. (Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification ~~but~~ for more than 10% but less than (or equal to) 15% of its ~~BES~~	The Responsible Entity did not implement any documented program(s) for access management. (Requirement R4) OR The Responsible Entity did not ~~implement one or more documented program(s) for access management that includes a process to~~ authorize electronic access or unescorted physical access~~. (~~ based on need for three or more individuals. (Part 4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters. ~~(~~(Part 4.2) OR The Responsible Entity ~~has implemented processes to~~did not verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		~~Systems~~BCS or SCI, privileges were incorrect or unnecessary. ~~(~~(Part 4.3)	~~Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. (Part 4.3)	verification ~~but~~ for more than 15% of its ~~BES Cyber Systems~~BCS or SCI, privileges were incorrect or unnecessary. ~~(~~(Part 4.3)
R5	The Responsible Entity ~~has implemented one or more process(es) to~~ did not revoke ~~the~~ individual’s user accounts upon termination action ~~but did not do so for~~ within 30 calendar days of the date of termination action for one or more individuals. (Part 5.3) OR The Responsible Entity ~~has implemented one or more process(es) to~~did not change passwords for shared accounts known to the user upon termination action, reassignment, or transfer~~, but did not do so for~~ within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals. (Part 5.4) OR	The Responsible Entity ~~has implemented one or more process(es) to remove the~~ did not initiate removal of the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for one individual. (Part 5.1) OR ~~The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~The Responsible Entity for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by	The Responsible Entity ~~has implemented one or more process(es) to remove the~~ did not initiate removal of the ability for unescorted physical access and ~~Interactive Remote Access~~IRA upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for two individuals. (Part 5.1) OR ~~The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~The Responsible Entity for two individuals, did not revoke the authorized	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access or unescorted physical access. (Requirement R5) OR The Responsible Entity ~~has implemented one or more process(es) to remove~~did not initiate removal of the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action ~~but did not initiate those removals~~ for three or more individuals. (Part 5.1) OR ~~The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,~~The

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but~~The Responsible Entity did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances. (Part 5.4)	the end of the next calendar day following the predetermined date. (Part 5.2)	electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)	Responsible Entity for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date. (Part 5.2)
R6	The Responsible Entity~~ has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for one individual, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. ~~(~~(Part 6.1) OR The Responsible Entity ~~performed~~did not perform the verification required by ~~Requirement R6~~ Part 6.2 ~~more~~	The Responsible Entity~~ has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for two individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. ~~(~~(Part 6.1) OR The Responsible Entity ~~performed~~did not perform the verification required by	The Responsible Entity~~ has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for three individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. ~~(~~(Part 6.1) OR The Responsible Entity ~~performed~~did not perform the verification required by	The Responsible Entity did not implement one or more documented access management program(s) for BCSI. ~~(~~(Requirement R6) OR The Responsible Entity~~ has implemented one or more program(s) as required by Requirement R6 Part 6.1 but~~, for four or more individuals, did not authorize provisioned electronic access to electronic BCSI or provisioned physical access to physical BCSI. ~~(~~(Part 6.1)

R #	Violation Severity Levels (CIP-004-~~7~~8)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~than~~within 15 calendar months but did in less than or equal to 16 calendar months of the previous verification. ~~(~~(Part 6.2) OR The Responsible Entity ~~has implemented~~, for one ~~or more program(s) to~~individual, did not remove the individual's ability to use provisioned access to BCSI ~~but, for one individual, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	~~Requirement R6~~ Part 6.2 ~~more than~~within 16 calendar months but did in less than or equal to 17 calendar months of the previous verification. ~~(~~(Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to~~, for two individuals, did remove ~~the~~each individual's ability to use provisioned access to BCSI ~~but, for two individuals, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	~~Requirement R6~~ Part 6.2 ~~more than~~within 17 calendar months but less than or equal to 18 calendar months of the previous verification. ~~(~~(Part 6.2) OR The Responsible Entity ~~has implemented one or more program(s) to~~, for three individuals, did not remove ~~the~~each individual's ability to use provisioned access to BCSI ~~but, for three individuals, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.	OR The Responsible Entity ~~performed~~did not perform the verification required by ~~Requirement R6~~ Part 6.2 more than 18 calendar months of the previous verification. ~~(~~(Part 6.2) OR The Responsible Entity ~~has implemented one~~, for four or more ~~program(s) to~~individuals, did not remove ~~the~~each individual's ability to use provisioned access to BCSI ~~but, for four or more individuals, did not do so~~ by the timeframe required in ~~Requirement R6,~~ Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- ~~None.~~Implementation Plan for Project 2016-02
- CIP-004-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-004-5.	
5.1	9/30/13	Modified two VSLs in R4	Errata
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct

Version	Date	Action	Change Tracking
			language and communication networks.
6	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-004-6. Docket No. RM15-14-000	
7	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
~~7~~8	~~12/7/21~~TBD	~~FERC Order issued approving CIP-004-7~~ ~~Docket No. RD21-6-000~~Modified by Project 2016-02.	
~~7~~	~~12/10/21~~	~~Effective Date~~	~~1/1/24~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29, 2023

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 CIP Definitions".

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-8

3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1. Balancing Authority

    4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3. Generator Operator

    4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **"Applicable Systems":** Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. **Effective Date:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP.	Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Systems connected via a routable protocol within each ESP.
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration).

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that control an ESP for an Applicable System in Part 1.1	Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.	Examples of evidence may include, but are not limited to, documentation of the methods implemented to permit only needed network accessibility to Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the Management Interfaces (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).
1.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious routable protocol communications detection methods (e.g., intrusion detection system, application layer firewall, etc.) are implemented.

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High impact BCS and their associated PCA Medium impact BCS at Control Centers and their associated PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time-sensitive communication of Protection Systems.	Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Permit Interactive Remote Access (IRA), if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	Intermediate System(s) used to access an Applicable System in Part 2.1	Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Examples of evidence may include, but are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption) initiate and terminate.
2.3	Intermediate System(s) used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Example of evidence may include, but are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID;

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			- Something the individual has such as tokens, digital certificates, or smart cards; or - Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
2.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, including IRA and system-to-system remote access, such as: - Methods for accessing logged or monitoring information to determine active vendor remote access sessions; - Methods for monitoring activity (e.g., connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g., netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or - Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High impact BCS and their associated PCA	Have one or more method(s) to	Examples of evidence may include,

CIP-005-8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	disable active vendor remote access (including IRA and system-to-system remote access).	but are not limited to, documentation of the methods(s) used to disable active vendor remote access • (including IRA and system-to-system remote access).
2.6	Intermediate System(s) used to access an Applicable System in Part 2.1	Prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System and supporting Cyber Systems.
2.7	Intermediate System(s) used to access an Applicable System in Part 2.1	Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Network diagrams of Intermediate Systems architecture; or • Configuration, settings, or policy of the EAP which controls routable protocol communications of IRA through the ESP.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part .	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part.	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. **Compliance Enforcement Authority:** "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. **Evidence Retention:** The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. **Compliance Monitoring and Enforcement Program:** As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td>R1.</td><td></td><td></td><td>The Responsible Entity did not have a method for detecting known or suspected malicious routable protocol communications entering or leaving the ESP required by Part 1.5.
OR
The Responsible Entity did not document the reason for permitting communications. (Part 1.2)</td><td>The Responsible Entity did not document one or more processes for CIP-005-8 Table R1 – Electronic Security Perimeter. (R1)
OR
The Responsible Entity did not protect the Applicable Systems connected to the network with routable protocol with an ESP. (Part 1.1)
OR
The Responsible Entity did not permit only needed communications and deny all other communications, through the ESP; excluding time sensitive communications of Protection Systems. (Part 1.2)
OR
The Responsible Entity did not protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces for Applicable</td></tr>
</table>

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td></td><td>Systems per system capability. (Part 1.3)
OR
The Responsible Entity did not perform authentication when establishing Dial-up Connectivity with the Applicable Systems. (Part 1.4)
OR
The Responsible Entity did not implement a method to protect the data traversing communication links, used to span a single ESP between PSPs, as required by Part 1.6.</td></tr>
<tr><td>R2.</td><td>The Responsible Entity does not have documented processes for one or more of the applicable Requirement Parts 2.1 through 2.3.</td><td>The Responsible Entity did not implement processes for one of the applicable Requirement Parts 2.1 through 2.3.</td><td>The Responsible Entity did not implement processes for two of the applicable Requirement Parts 2.1 through 2.3.
OR
The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access</td><td>The Responsible Entity did not implement processes for three of the applicable Requirement Parts 2.1 through 2.3.
OR
The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote access</td></tr>
</table>

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			(including IRA and system-to-system remote access) (Part 2.5).	(including IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not prevent Intermediate System(s) from sharing CPU resources or memory resources with any part of a high or medium impact BCS or associated PCAs. (Part 2.6). OR The Responsible Entity did not ensure routable protocol communications from an Intermediate System to high or medium impact BCS or associated PCAs went through an ESP (Part 2.7).
R3.	The Responsible Entity did not document one or more processes for CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI. (Requirement R3)	The Responsible Entity did not have a method to determine authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.1). OR	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity did not have a method to determine authenticated vendor-initiated	The Responsible Entity did not implement any processes for CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI. (Requirement R3) OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections for PACS or SCI supporting PACS (Part 3.2).	remote connections for EACMS or SCI supporting EACMS (Part 3.1). OR The Responsible Entity did not have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS or SCI supporting EACMS (Part 3.2).	The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-005-8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
7	11/05/2020	Adopted by the NERC Board of Trustees.	
7	03/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
7	4/5/2021	Effective Date	10/1/2022
8	TBD	Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29, 2023

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 ~~Draft 5~~CIP Definitions".

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-8

3. **Purpose:** To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

        4.1.1. Balancing Authority

        4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

            4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

                4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

                4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

            4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

            4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

            4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

        4.1.3. Generator Operator

        4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-8:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BCS categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies.

5. Effective Date: See "Project 2016-02 Modifications to CIP Standards Implementation Plan."

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA	~~All applicable Cyber Assets~~Applicable Systems connected to a network via a routable protocol ~~shall reside within a defined~~must be protected by an ESP.	~~An example~~Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber ~~Assets~~Systems connected via a routable protocol within each ESP.
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
			configuration).
1.3	SCI supporting an Applicable System from Part 1.1. EACMS, and their supporting SCI, that control an ESP for an Applicable System in Part 1.1	Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.	Examples of evidence may include, but are not limited to, documentation of the methods implemented to permit only needed network accessibility to Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the Management Interfaces (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).
1.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious routable protocol communications detection methods (e.g., intrusion detection system, application

CIP-005-~~7~~8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
			layer firewall, etc.) are implemented.
1.~~2~~6	High ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS at Control Centers and their associated~~:~~ PCA	~~All External Routable Connectivity must be through an identified Electronic Access Point (EAP).~~Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ~~i.~~ii. Time-sensitive communication of Protection Systems.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, ~~network diagrams showing all external routable communication paths~~documentation of methods used to protect the confidentiality and integrity of the ~~identified EAPs.~~ data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).

~~CIP-005-7 Table R1 – Electronic Security Perimeter~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~

~~**1.3**~~	~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems~~	~~Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.~~	~~An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.~~
~~**1.4**~~	~~High Impact BES Cyber Systems with Dial-up Connectivity and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated:~~ ~~• PCA~~	~~Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.~~	~~An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.~~
~~**1.5**~~	~~Electronic Access Points for High Impact BES Cyber Systems~~ ~~Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers~~	~~Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.~~	~~An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.~~

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, ~~where technically feasible~~per system capability, in *CIP-005-~~7~~8 Table R2 – Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~7~~8 Table R2 – Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~impact BCS and their associated~~:~~ PCA SCI supporting an Applicable System in this Part	~~For all~~Permit Interactive Remote Access~~, utilize~~ (IRA), if any, only through an Intermediate System~~ such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~.	Examples of evidence may include, but are not limited to, network diagrams~~ or~~, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~PCA~~Intermediate System(s) used to access an Applicable System in Part 2.1	~~For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.~~Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption ~~initiates~~) initiate and ~~terminates.~~ terminate.

CIP-005-~~7~~8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	~~High Impact BES Cyber Systems and their associated:~~ ~~• PCA~~ ~~Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:~~ ~~• PCA~~ Intermediate System(s) used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for ~~all~~ ~~Interactive Remote Access sessions~~IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	~~An example~~Example of evidence may include, but ~~is~~are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.
2.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ ~~•~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~ impact BCS and their associated~~:~~ ~~•~~ PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access, ~~(~~including ~~Interactive Remote Access~~ IRA and system-to-system remote access~~),~~ , such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions;

CIP-005-~~7~~8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Methods for monitoring activity (e.g~~.~~., connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g~~.~~., netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.
2.5	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ PCA Medium ~~Impact BES Cyber Systems with External Routable Connectivity~~ impact BCS and their associated~~:~~ PCA SCI supporting an Applicable System in this Part	Have one or more method(s) to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including ~~Interactive Remote Access~~ IRA and system-to-system remote access~~),~~ ~~such as:~~ • ~~Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or~~ • ~~Methods to disable vendor Interactive Remote Access at~~

CIP-005-~~7~~8 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			~~the applicable Intermediate System.~~).
2.6	Intermediate System(s) used to access an Applicable System in Part 2.1	Prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System and supporting Cyber Systems.
2.7	Intermediate System(s) used to access an Applicable System in Part 2.1	Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Network diagrams of Intermediate Systems architecture; or • Configuration, settings, or policy of the EAP which controls routable protocol communications of IRA through the ESP.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-~~7~~8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and ~~PACS~~SCI*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS~~SCI

Part	Applicable Systems	Requirements	Measures
3.1	EACMS and PACS associated with ~~High Impact BES Cyber Systems~~ high impact BCS. EACMS and PACS associated with ~~Medium Impact BES Cyber Systems~~medium impact BCS with ~~External Routable Connectivity~~ ERC. SCI supporting an Applicable System in this Part .	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.
3.2	EACMS and PACS associated with ~~High Impact BES Cyber Systems~~high impact BCS. EACMS and PACS associated with ~~Medium Impact BES Cyber Systems~~medium impact BCS with ~~External Routable Connectivity~~ ERC. SCI supporting an Applicable System in this Part.	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a

CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS~~SCI			
Part	Applicable Systems	Requirements	Measures
			firewall; or physically disconnecting a network cable to prevent a reconnection.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1.			The Responsible Entity did not have a method for detecting known or suspected malicious routable protocol communications entering or leaving the ESP required by Part 1.5. OR The Responsible Entity did not document the reason for ~~both inbound and outbound~~permitting communications. (Part 1.~~5)~~2)	The Responsible Entity did not document one or more processes for *CIP-005-~~6~~8 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not ~~have all applicable Cyber Assets~~protect the Applicable Systems connected to ~~a~~the network ~~via a~~with routable protocol ~~within a defined Electronic Security Perimeter (ESP). (~~with an ESP. (Part 1.1) OR ~~External Routable Connectivity through the ESP was not through an identified EAP. (1.2)~~ ~~OR~~ The Responsible Entity did not ~~require inbound and outbound access permissions~~permit only needed communications and deny all other

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~access~~communications, through the ESP; excluding time sensitive communications of Protection Systems. (Part 1.2) OR The Responsible Entity did not protect ESP and SCI configurations by ~~default.~~ ~~(~~implementing methods to permit only needed network accessibility to Management Interfaces for Applicable Systems per system capability. (Part 1.3) OR The Responsible Entity did not perform authentication when establishing ~~dial~~Dial-up ~~connectivity with the applicable Cyber Assets, where technically feasible.~~ ~~(~~Connectivity with the Applicable Systems. (Part 1.4) OR The Responsible Entity did not implement a method to protect the data traversing communication links, used to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				span a single ESP between PSPs, as required by Part 1.6.
R2.	The Responsible Entity does not have documented processes for one or more of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.4); or one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5).	The Responsible Entity did not implement processes for three of the applicable ~~items for~~ Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including ~~Interactive Remote Access~~ IRA and system-to-system remote access) (Part 2.4) and one or more methods to disable active vendor remote access (including ~~Interactive Remote Access~~IRA and system-to-system remote access) (Part 2.5). OR The Responsible Entity did not prevent Intermediate System(s) from sharing CPU resources or memory resources with any part of

R #	**Violation Severity Levels**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
				a high or medium impact BCS or associated PCAs. (Part 2.6). OR The Responsible Entity did not ensure routable protocol communications from an Intermediate System to high or medium impact BCS or associated PCAs went through an ESP (Part 2.7).
R3.	The Responsible Entity did not document one or more processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS.~~ ~~(~~SCI.* (Requirement R3)	The Responsible Entity ~~had method(s) as required by Part 3.1 for EACMS but~~ did not have a method to determine authenticated vendor-initiated remote connections for PACS ~~(~~or SCI supporting PACS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for EACMS but~~ did not have a method to terminate authenticated vendor-initiated remote connections for PACS ~~(3.2~~or SCI supporting PACS (Part 3.2).	The Responsible Entity did not implement processes for either Part 3.1 or Part 3.2. (Requirement R3) OR The Responsible Entity ~~had method(s) as required by Part 3.1 for PACS but~~ did not have a method to determine authenticated vendor-initiated remote connections for EACMS ~~(~~or SCI supporting EACMS (Part 3.1). OR The Responsible Entity ~~had method(s) as required by Part 3.2 for PACS but~~ did not	The Responsible Entity did not implement any processes for *CIP-005-~~7~~8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and ~~PACS.~~ ~~(~~SCI.* (Requirement R3) OR The Responsible Entity did not have any methods as required by Parts 3.1 and 3.2 (Requirement R3).

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			have a method to terminate authenticated vendor-initiated remote connections or control the ability to reconnect for EACMS ~~(~~or SCI supporting EACMS (Part 3.2).	

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-005-~~7~~8 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	
6	10/18/2018	FERC Order approving CIP-005-6. Docket No. RM17-13-000.	
7	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
7	11/05/2020	Adopted by the NERC Board of Trustees.	
7	~~3~~03/18/2021	FERC Order approving CIP-005-7. Docket No. RD21-2-000	
7	4/5/2021	Effective Date	10/1/2022
8	TBD	Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 33, 2022

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 CIP Definitions"

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific Requirement Part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium impact BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium impact BCS with ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access, per system capability.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Monitor for unauthorized access through a physical access point into a PSP.	Examples of evidence may include, but are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a PSP.
1.5	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a PSP and additional evidence that the alarm or alert was issued and communicated as identified in the Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Monitor each PACS for unauthorized physical access to a PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	PACS associated with: - High impact BCS, or - Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.
1.8	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each PSP, with information to identify the individual and date and time of entry.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes logging and recording of physical entry into each PSP and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each PSP that show the individual and the date and time of entry into each PSP.

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days.	Examples of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP that show the date and time of entry into each PSP.

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each PSP.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require manual or automated logging of visitor entry into and exit from each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain visitor logs for at least 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	PACS associated with: • High impact BCS, or • Medium impact BCS with ERC Locally mounted hardware or devices at the PSP associated with: • High impact BCS, or • Medium impact BCS with ERC	Maintenance and testing of each PACS and locally mounted hardware or devices at each PSP at least once every 24 calendar months to ensure they function properly.	Examples of evidence may include, but are not limited to, a maintenance and testing program that provides for testing each PACS and locally mounted hardware or devices associated with each applicable each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention: The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Part 1.3) OR The Responsible Entity does not have a process to monitor

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				for unauthorized access through a physical access point into a PSP. (Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each PACS for unauthorized physical access to a PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log

<table>
<tr><th rowspan="2">R #</th><th colspan="4">Violation Severity Levels (CIP-006-7)</th></tr>
<tr><th>Lower VSL</th><th>Moderate VSL</th><th>High VSL</th><th>Severe VSL</th></tr>
<tr><td></td><td></td><td></td><td></td><td>authorized physical entry into each PSP with sufficient information to identify the individual and date and time of entry. (Part 1.8)
OR
The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9)</td></tr>
<tr><td>**R2**</td><td>N/A</td><td>N/A</td><td>N/A</td><td>The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1)
OR
The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor’s name, and the point of contact. (Part 2.2)
OR
The Responsible Entity failed to include or implement a</td></tr>
</table>

R #	Violation Severity Levels (CIP-006-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				visitor control program to retain visitor logs for at least 90 days. (Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for PACS and locally mounted hardware or devices at the PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for PACS and locally mounted hardware or devices at the PSP, but did not complete required testing within 27 calendar months. (Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-006-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 33, 2022

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 ~~Draft 4~~CIP Definitions"

A. Introduction

1. **Title:** Cyber Security — Physical Security of BES Cyber Systems

2. **Number:** CIP-006-~~6~~7

3. **Purpose:** To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~4.1.6~~4.1.5 Reliability Coordinator

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-006-~~6~~7:

4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between Cyber Systems, providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5.1~~ identification and categorization processes.

~~**5. Effective Dates:**~~

~~See Implementation Plan for CIP-006-6.~~

~~**6. Background:**~~

~~Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the~~

~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

4.3. “Applicable Systems~~” **Columns in Tables:**~~”: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific ~~requirement row~~Requirement Part applies. ~~The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

- ~~**Medium Impact BES Cyber Systems without External Routable Connectivity –** Only applies to medium impact BES Cyber Systems without External Routable Connectivity.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity –** Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS) –** Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~
- ~~**Physical Access Control Systems (PACS) –** Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~
- ~~**Protected Cyber Assets (PCA) –** Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

5. ~~**Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.~~

Effective Dates: See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-~~6~~7 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-~~6~~7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-~~6~~7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium ~~I~~impact ~~BES cyber Systems~~ BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High i~~I~~mpact ~~BES Cyber Systems~~BCS, or • Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	~~An example~~Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.

CIP-006-~~6~~7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.2	Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable ~~Physical Security Perimeter~~PSP to only those individuals who have authorized unescorted physical access.	~~An example~~Examples of evidence may include, but are not limited to, language in the physical security plan that describes each ~~Physical Security Perimeter~~PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.
1.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA -SCI supporting an Applicable System in this Part	~~Where technically feasible, utilize~~Utilize two or more different physical access controls (this does not require two completely independent ~~physical access control systems~~PACS) to collectively allow unescorted physical access into ~~Physical Security Perimeters~~PSPs to only those individuals who have authorized unescorted physical access~~.~~ , per system capability.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, language in the physical security plan that describes ~~the Physical Security Perimeters~~each PSP and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-~~6~~7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.4	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~ PSP.	Examples ~~An example~~ of evidence may include, but are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter~~ PSP.
1.5	High i~~I~~mpact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~ PSP to the personnel identified in the ~~BES~~ Cyber Security Incident response plan within 15 minutes of detection.	Examples ~~An example~~ of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a ~~Physical Security Perimeter~~ PSP and additional evidence that the alarm or alert was issued and communicated as identified in the ~~BES~~ Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

CIP-006-~~6~~7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	Physical Access Control Systems (PACS) associated with: • High i~~I~~mpact ~~BES Cyber Systems~~ BCS, or • Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC SCI supporting an Applicable System in this Part	Monitor each ~~Physical Access Control System~~ PACS for unauthorized physical access to a ~~Physical Access Control System~~ PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.
1.7	~~Physical Access Control Systems (~~PACS~~)~~ associated with: • High i~~I~~mpact ~~BES Cyber Systems~~BCS, or • Medium i~~I~~mpact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized physical access to a ~~Physical Access Control System~~ PACS to the personnel identified in the ~~BES~~ Cyber Security Incident response plan within 15 minutes of the detection.	Examples ~~An example~~ of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to ~~Physical Access Control Systems~~ PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-~~6~~7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High i~~I~~mpact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each ~~Physical Security Perimeter~~PSP, with information to identify the individual and date and time of entry.	Examples ~~An example~~ of evidence may include, but are not limited to, language in the physical security plan that describes logging and recording of physical entry into each PSP ~~Physical Security Perimeter~~ and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each PSP ~~Physical Security Perimeter~~ that show the individual and the date and time of entry into each PSP ~~Physical Security Perimeter~~.
1.9	High i~~I~~mpact BCS ~~BES Cyber Systems~~ and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact BCS ~~BES Cyber Systems~~ with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP ~~Physical Security Perimeter~~ for at least 90 calendar days.	Examples ~~An example~~ of evidence may include, but are not limited to, dated documentation such as logs of physical access into each PSP ~~Physical Security Perimeter~~ that show the date and time of entry into each PSP~~Physical Security Perimeter~~.

~~1.10~~	~~High Impact BES Cyber Systems and their associated:~~ • ~~PCA~~ ~~Medium Impact BES Cyber Systems at Control Centers and their associated:~~ ~~PCA~~	~~Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.~~ ~~Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:~~ • ~~encryption of data that transits such cabling and components; or~~ • ~~monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or~~ • ~~an equally effective logical protection.~~	~~An example of evidence may include, but is not limited to, records of the Responsible Entity's implementation of the physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays) encryption, monitoring, or equally effective logical protections.~~

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-~~6~~7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-~~6~~7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~6~~7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each ~~Physical Security Perimeter, except during CIP Exceptional Circumstances.~~PSP.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, language in a visitor control program that requires continuous escorted access of visitors within ~~Physical Security Perimeters~~each PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.
2.2	High i~~I~~mpact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; and 2. PCA Medium i~~I~~mpact ~~BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ ERC and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from each ~~Physical Security Perimeter~~ PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor~~, except during CIP Exceptional Circumstances~~.	Examples ~~An example~~ of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each ~~Physical Security Perimeter~~ PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

	SCI supporting an Applicable System in this Part		

CIP-006-~~6~~7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain visitor logs for at least 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least 90 calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-~~6~~7 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-~~6~~7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-~~6~~7 Table R3 – Physical Access Control System Maintenance and Testing Program

Part	Applicable Systems	Requirement	Measures
3.1	~~Physical Access Control Systems (~~PACS~~)~~ associated with: • High ~~Impact BES Cyber Systems~~impact BCS, or • Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC Locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP associated with: • High ~~Impact BES Cyber Systems~~impact BCS, or • Medium ~~Impact BES Cyber Systems~~impact BCS with ~~External Routable Connectivity~~ERC	Maintenance and testing of each ~~Physical Access Control System~~PACS and locally mounted hardware or devices at ~~the Physical Security Perimeter~~each PSP at least once every 24 calendar months to ensure they function properly.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, a maintenance and testing program that provides for testing each ~~Physical Access Control System~~PACS and locally mounted hardware or devices associated with each applicable ~~Physical Security Perimeter~~each PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

~~**1.1.**~~ **Compliance Enforcement Authority:**

~~1.2.~~1.1. As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

~~**1.3.**~~ **Evidence Retention:**

1.2. The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

~~**1.4.**~~ **Compliance Monitoring and Assessment Processes:**

~~1.5.~~1.3. As defined in the NERC Rules of Procedure, "Compliance ~~Audits~~Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Investigations~~

~~Self-Reporting~~

~~Complaints~~

~~**1.6. Additional Compliance Information:**~~

~~None~~

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-006-~~6~~7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
R1	N/A	N/A	N/A	The Responsible Entity did not document or implement physical security plans. (Requirement R1) OR The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (Part 1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (Part 1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (Part 1.3) OR

R #	Violation Severity Levels (CIP-006-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a ~~Physical Security Perimeter. (~~PSP. (Part 1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a ~~Physical Security Perimeter~~PSP or to communicate such alerts within 15 minutes to identified personnel. (Part 1.5) OR The Responsible Entity does not have a process to monitor each ~~Physical Access Control System~~PACS for unauthorized physical access to a ~~Physical Access Control Systems. (~~PACS. (Part 1.6) OR The Responsible Entity does not have a process to alert for

R #	Violation Severity Levels (CIP-006-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				unauthorized physical access to ~~Physical Access Control Systems~~PACS or to communicate such alerts within 15 minutes to identified personnel. (Part 1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each ~~Physical Security Perimeter~~PSP with sufficient information to identify the individual and date and time of entry. (Part 1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (Part 1.9) ~~OR~~ ~~The Responsible Entity did not document or implement physical access restrictions, encryption, monitoring or equally effective logical~~

R #	Violation Severity Levels (CIP-006-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~protections for cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (1.10)~~
R2	N/A	N/A	N/A	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (Part 2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the

R #	Violation Severity Levels (CIP-006-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				visitor's name, and the point of contact. (Part 2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ~~ninety~~90 days. (Part 2.3)
R3	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (Part 3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (Part 3.1)	The Responsible Entity did not document or implement a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter. (~~PSP. (Part 3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for ~~Physical Access Control Systems~~PACS and locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP, but did not complete required

R #	Violation Severity Levels (CIP-006-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				testing within 27 calendar months. (Part 3.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

~~None.~~

- Implementation Plan for Project 2016-02
- CIP-006-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-006-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791.
6	1/21/16	FERC order issued approving CIP-006-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~General:~~

~~While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.~~

~~Requirement R1:~~

~~Methods of physical access control include:~~

- ~~Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~
- ~~Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~
- ~~Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~

- ~~Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the Physical Security Perimeter.~~

~~Methods to monitor physical access include:~~

- ~~Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.~~
- ~~Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.~~

~~Methods to log physical access include:~~

- ~~Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.~~
- ~~Video Recording: Electronic capture of video images of sufficient quality to determine identity.~~
- ~~Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.~~

~~The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.~~

~~Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.~~

~~The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the~~

~~physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.~~

~~This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where this cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.~~

~~The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.~~

~~The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.~~

~~The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be~~

~~implemented on third-party components when entities rely on leased third-party communications.~~

~~In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.~~

~~Requirement R2:~~

~~The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.~~

~~The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.~~

~~Requirement R3:~~

~~This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a Physical Security Perimeter (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.~~

~~Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center's communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable~~

~~communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.~~

~~**Rationale for Requirement R2:**~~

~~To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.~~

~~**Rationale for Requirement R3:**~~

~~To ensure all Physical Access Control Systems and devices continue to function properly.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29, 2023

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed new or modified terms titled “Project 2016-02 CIP Definitions.”

A. Introduction

1. **Title:** Cyber Security — System Security Management
2. **Number:** CIP-007-7
3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1 Balancing Authority

    4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002- identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See Project 2016-02 Modifications to CIP Standards Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports or network accessible logical services, individually or by group; • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; • Configuration or settings of host-based firewalls or other device level mechanisms that disable or prevent unneeded network accessible logical ports or network accessible logical services; or • Identity or process based access policy or workload configuration demonstrating needed network accessibility.

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium impact BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Examples of evidence may include, but are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting either: High impact BCS or their associated PCA. Medium impact BCS or their associated PCA.	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Cyber Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.	Examples of evidence may include, but are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.
2.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Examples of evidence may include, but are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security patches released by the documented sources at least once every 35 calendar days.

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: - Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of component software revision, or registry exports that show software has been installed); or - A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.
2.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Examples of evidence may include, but are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R3 – Malicious Code Prevention

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of evidence may include, but are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Examples of evidence may include, but are not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events, per system capability: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use.
5.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify individuals who have authorized access to shared accounts.	Examples of evidence may include, but are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: - Records of a procedure that passwords are changed when new devices are in production; or - Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: - System-generated reports or screenshots of the system-enforced password parameters, including length and complexity; or - Attestations that include a reference to the documented procedures that were followed.

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.
5.7	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information:

None

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)	The Responsible Entity had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS. (Part 1.3)	The Responsible Entity neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity did not evaluate the cyber security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	The Responsible Entity did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR	The Responsible Entity did not include any processes for installing cyber security patches for Applicable Systems. (Part 2.1) OR The Responsible Entity did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-7 Table R2. (Requirement R2) OR The Responsible Entity did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		The Responsible Entity did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	an existing mitigation plan within 65 calendar days of the evaluation completion. (Part 2.3)	OR The Responsible Entity did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)
R3	N/A	The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3). OR The Responsible Entity did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity missed one of 15 calendar day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	The Responsible Entity missed one 15 calendar day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	The Responsible Entity did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity missed two or more 15 calendar day intervals. (Part 4.4)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity, per system capability, did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3) OR The Responsible Entity did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity process(es) for password-only authentication for interactive user access did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity did not, per device capability, change known default passwords. (Part 5.4) OR The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity did not technically or procedurally enforce password changes or an obligation to change the

R #	Violation Severity Levels (CIP-007-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity neither limited the number of unsuccessful authentication attempts nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-007-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses

Version	Date	Action	Change Tracking
			remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the ~~fifth~~ final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29, 2023

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed new or modified terms titled “Project 2016-02 ~~Draft 5~~CIP Definitions.”

A. Introduction

1. **Title:** Cyber Security — System Security Management

2. **Number:** CIP-007-~~6~~7

3. **Purpose:** To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System (SPS) or~~ Remedial Action Scheme (RAS) where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~4.1.6~~4.1.5 Reliability Coordinator

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~SPS or~~ RAS where the ~~SPS or~~ RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-~~6~~7:

4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

~~4.2.3.2~~4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-~~5.1~~ identification and categorization processes.

~~5. Effective Dates:~~

~~See Implementation Plan for CIP-007-6.~~

~~6. Background:~~

~~Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, “~~*~~Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].”~~* ~~The referenced table requires the applicable items in the procedures for the requirement’s common subject matter.~~

~~The term~~ *~~documented processes~~* ~~refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms~~ *~~program~~* ~~and~~ *~~plan~~* ~~are sometimes used in place of~~ *~~documented processes~~* ~~where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as~~ *~~plans~~* ~~(i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~” Columns in Tables:~~

~~5.1.~~4.3. ”: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies. ~~The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~

- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.~~
- ~~**Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

5. ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~**Effective Dates:** See Project 2016-02 Modifications to CIP Standards Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R1 – ~~Ports and Services~~System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R1 – ~~Ports and Services~~System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control~~Medium Impact BES Cyber~~ Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA	~~Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.~~Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports ~~on all applicable Cyber Assets and Electronic Access Points, individually~~ or ~~by group.~~network accessible logical services, individually or by group; • Listings of the listening ports ~~on the Cyber Assets~~, individually or by group, from either ~~the device~~ configuration files or settings, command output (such as netstat), or network scans of open ports; ~~or~~

CIP-007-~~6~~7 Table R1– ~~Ports and Services~~System Hardening

Part	Applicable Systems	Requirements	Measures
	SCI supporting an Applicable System in this Part.		• Configuration ~~files~~or settings of host-based firewalls or other device level mechanisms that ~~only allow~~disable or prevent unneeded network accessible logical ports or network accessible logical services; or • Identity or process based access policy or workload configuration demonstrating needed ~~ports and deny all others.~~ network accessibility.

CIP-007-~~6~~7 Table R1– ~~Ports and Services~~System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
1.3	SCI supporting either: High impact BCS or their associated PCA. Medium impact BCS or their associated PCA.	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.1	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	A patch management process for tracking, evaluating, and installing cyber security patches ~~for applicable Cyber Assets~~. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for ~~applicable Cyber Assets~~Applicable Systems that are updateable and for which a patching source exists.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored~~, whether on an individual BES Cyber System or Cyber Asset basis.~~ .
2.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated:	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security~~-related~~ patches released by the documented sources at least once every 35 calendar days.

CIP-007-~~6~~7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.		
2.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; ~~or~~ - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: - Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of ~~BES Cyber System Component~~component software revision, or registry exports that show software has been installed); or - A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.
2.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

CIP-007-~~6~~7 Table R2 – ~~Cyber~~ Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Manager or delegate.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R3 – Malicious Code Prevention

Part	Applicable Systems	Requirements	Measures
3.1	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Deploy method(s) to deter, detect, or prevent malicious code.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).
3.2	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

CIP-007-~~6~~7 Table R3 – Malicious Code Prevention

Part	Applicable Systems	Requirements	Measures
	BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.		
3.3	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R4 – Security Event Monitoring

Part	Applicable Systems	Requirements	Measures
4.1	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Log security events ~~at the BES Cyber System level (~~, per ~~BES Cyber System~~system capability~~) or at the Cyber Asset level (per Cyber Asset capability)~~, for identification of, and after-the-fact investigations of, Cyber Security Incidents that ~~includes, as~~include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the ~~BES Cyber~~Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.
4.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS with ~~External Routable~~	Generate alerts for security events that the Responsible Entity determines necessitates an alert~~,~~ that includes, as a minimum, each of the following types of events ~~(~~, per ~~Cyber Asset or BES Cyber System~~system capability~~):~~: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-~~6~~7 Table R4 – Security Event Monitoring

Part	Applicable Systems	Requirements	Measures
	~~Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	logging.	
4.3	High ~~I~~impact ~~BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~ BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	~~Where technically feasible, retain~~Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.
4.4	High ~~I~~impact ~~BES Cyber Systems~~ BCSand their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, ~~any~~ findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-~~6~~7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-~~6~~7 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.1	High ~~I~~impact~~ BES Cyber Systems~~ BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact~~ BES Cyber Systems~~ BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact~~ BES Cyber Systems~~ BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Have a method(s) to enforce authentication of interactive user access, ~~where technically feasible~~per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-~~6~~7 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.2	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use~~ for the BES Cyber System~~.
5.3	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify individuals who have authorized access to shared accounts.	~~An e~~Examples of evidence may include, but ~~is ~~are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-~~6~~7 Table R5 – System Access Control

Part	Applicable Systems	Requirements	Measures
5.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: - Records of a procedure that passwords are changed when new devices are in production; or - Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.
5.5	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems~~Cyber Asset~~; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable Systems~~Cyber Asset~~.	Examples of evidence may include, but are not limited to: - System-generated reports or screenshots of the system-enforced password parameters, including length and complexity; or - Attestations that include a reference to the documented procedures that were followed.

CIP-007-~~6~~7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	~~Where technically feasible, f~~For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: - System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or - Attestations that include a reference to the documented procedures that were followed.
5.7	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	~~Where technically feasible, either:~~ Limit the number of unsuccessful authentication attempts~~;~~ or ~~G~~generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: - Documentation of the account-lockout parameters; or - Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Compliance Violation Investigations~~

~~Self-Reporting~~

~~Complaints~~

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4. Additional Compliance Information:

None

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	~~R1~~The Responsible Entity did not document one or more process(es) that included the applicable items in CIP-007-7 Table R1. (Requirement R1)	The Responsible Entity ~~has implemented and documented processes for Ports and Services but~~ had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media. (Part 1.2)	The Responsible Entity ~~has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,~~ had one or more unneeded logical network accessible ports or network accessible services enabled. (Part 1.1) OR The Responsible Entity has not prevented the sharing of the CPU and memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS. (Part 1.3)	The Responsible Entity ~~did not implement or document~~neither implemented nor documented one or more process(es) that included the applicable items in CIP-007-6 Table R1. (Requirement R1)
R2	The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security~~	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes,	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-~~6~~7 Table R2. (Requirement R2) OR

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~patches for applicability but~~ did not evaluate the cyber security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion. (Part 2.3)	including the identification of sources, for tracking or evaluating cyber security patches for ~~applicable Cyber Assets. (~~Applicable Systems. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable	installing cyber security patches for ~~applicable Cyber Assets. (~~Applicable Systems. (Part 2.1) OR The Responsible Entity ~~has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but~~ did not evaluate the cyber security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified. (Part 2.2) OR The Responsible Entity ~~has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches,~~ did not apply the applicable cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the	The Responsible Entity ~~has documented or implemented one or more process(es) for patch management but~~ did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets. (Part 2.1) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but~~ did not obtain approval by the CIP Senior Manager or delegate. (Part 2.4) OR The Responsible Entity ~~documented a mitigation plan for an applicable cyber security patch but~~ did not implement the plan as created or revised within the timeframe specified in the plan. (Part 2.4)

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		cyber security patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion. (Part 2.3)	evaluation completion. (Part 2.3)	
R3	N/A	The Responsible Entity ~~has implemented one or more documented process(es), but~~, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns. (Part 3.3)	The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not mitigate the threat of detected malicious code. (Part 3.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention, but~~, where signatures or patterns are used, the Responsible Entity did not update malicious code protections. (Part 3.3).	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R3. (Requirement R3). OR The Responsible Entity ~~has implemented one or more documented process(es) for malicious code prevention but~~ did not deploy method(s) to deter, detect, or prevent malicious code. (Part 3.1)
R4	The Responsible Entity ~~has documented and~~	The Responsible Entity ~~has documented and~~	The Responsible Entity ~~has documented and~~	The Responsible Entity did not implement or document one or more process(es) that included

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~implemented~~ missed one ~~or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling~~ of ~~logged events at least every~~ 15 calendar ~~days but missed an~~day interval and completed the review within 22 calendar days of the prior review. (Part 4.4)	~~implemented~~ missed one ~~or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every~~ 15 calendar ~~days but missed an~~day interval and completed the review within 30 calendar days of the prior review. (Part 4.4)	~~implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but~~ did not generate alerts for all of the required types of security events described in 4.2.1 through 4.2.2. (Part 4.2) OR The Responsible Entity ~~has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but~~ did not retain applicable security event logs for at least the last 90 consecutive days. (Part 4.3) OR The Responsible Entity ~~has documented and implemented one or more process(es) to identify~~	the applicable items in CIP-007-6 Table R4. (Requirement R4) OR The Responsible Entity ~~has documented and implemented one or more process(es) to log events for the Applicable Systems (~~, per ~~device or~~ system capability~~)~~ ~~but~~, did not detect and log all of the required types of events described in 4.1.1 through 4.1.3. (Part 4.1)

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but~~ missed two or more 15 calendar day intervals. (Part 4.4)	
R5	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change. (Part 5.6)	The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). (Part 5.2) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~ did not include the identification of the individuals with authorized access to shared accounts. (Part 5.3)	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in CIP-007-6 Table R5. (Requirement R5) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but, where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but,~~

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for interactive user access that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented~~ process(es) for password-only authentication for interactive user access ~~that~~ did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for password-only authentication for~~	~~where technically feasible,~~ does not have a method(s) to enforce authentication of interactive user access. (Part 5.1) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Controls but~~ did not, per device capability, change known default passwords. (Part 5.4) OR ~~The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the~~The Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2. (Part 5.5) OR The Responsible Entity ~~has implemented one or more documented process(es) for~~

R #	Violation Severity Levels (CIP-007-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change. (Part 5.6)	~~password-only authentication for interactive user access but~~ did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change. (Part 5.6) OR The Responsible Entity ~~has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit~~neither limited the number of unsuccessful authentication attempts ~~or generate~~nor generated alerts after a threshold of unsuccessful authentication attempts. (Part 5.7)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-007-7 Technical Rationale

~~None.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-007-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
6	2/15/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order

Version	Date	Action	Change Tracking
			No. 791 related to transient devices and low impact BES Cyber Systems.
6	1/21/16	FERC order issued approving CIP-007-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.~~

~~**1.1.** This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'~~

~~**1.2.** Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.~~

~~The protection of these ports can be accomplished in several ways including, but not limited to:~~

~~Disabling all unneeded physical ports within the Cyber Asset's configuration~~

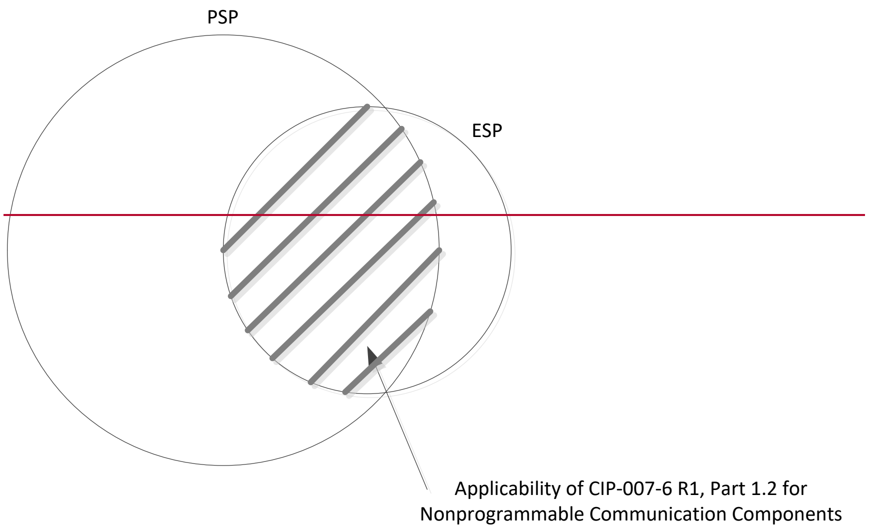
~~Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization~~

~~Physical port obstruction through removable locks~~

~~The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.~~

~~This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.~~

~~The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:~~



Location of Nonprogrammable Communication Components

~~Requirement R2:~~

~~The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.~~

~~Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.~~

~~One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.~~

~~2.1.~~ ~~The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they~~

~~can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.~~

~~**2.2.** Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.~~

~~When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.~~

~~**2.3.** The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or~~

~~those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.~~

~~**2.4.** The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.~~

~~**Requirement R3:**~~

~~**3.1.** Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.~~

~~**3.2.** When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or~~

~~method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.~~

~~Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media ("transient devices") in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.~~

~~**3.3.** In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.~~

~~**Requirement R4:**~~

~~Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.~~

~~**4.1.** In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.~~

~~Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.~~

~~User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.~~

~~It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.~~

~~**4.2.** Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.~~

~~The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:~~

~~Detected known or potential malware or malicious activity~~

~~Failure of security event logging mechanisms~~

~~Login failures for critical accounts~~

~~Interactive login of system accounts~~

~~Enabling of accounts~~

~~Newly provisioned accounts~~

~~System administration or change tasks by an unauthorized user~~

~~Authentication attempts on certain accounts during non-business hours~~

~~Unauthorized configuration changes~~

~~Insertion of Removable Media in violation of a policy~~

~~**4.3** Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.~~

~~**4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-~~

~~time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.~~

~~Requirement R5:~~

~~Account types referenced in this guidance typically include:~~

~~Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.~~

~~Individual user account: An account used by a single user.~~

~~Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.~~

~~System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.~~

~~Application account: A specific system account, with rights granted at the application level often used for access into a Database.~~

~~Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.~~

~~Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.~~

~~Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.~~

~~**5.1** Reference the Requirement's rationale.~~

~~**5.2** Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.~~

~~**5.3** Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.~~

~~**5.4.** Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.~~

~~The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or~~

~~installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.~~

~~**5.5.** Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.~~

~~Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.~~

~~**5.6** Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.~~

~~**5.7** Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.~~

~~Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.~~

~~In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.~~

~~The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).~~

~~Rationale for Requirement R2:~~

~~Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.~~

~~Rationale for Requirement R3:~~

~~Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.~~

~~Rationale for Requirement R4:~~

~~Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.~~

~~Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.~~

~~Rationale for Requirement R5:~~

~~To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.~~

~~Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.~~

~~Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.~~

~~Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.~~

~~Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.~~

~~For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.~~

~~The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.~~

~~The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.~~

~~The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled “Project 2016-02 CIP Definitions”.

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-7

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1 Balancing Authority

    4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the Bulk Electric System (BES):

    4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3 Generator Operator

    4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BES) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated Electronic Access Control and Monitoring Systems (EACMS) Medium impact BCS and their associated EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the Applicable Systems column for this Part; and 1.2.3 To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column including justification for attempt determination criteria and documented processes for notification.

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the Applicable Systems column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	Examples of evidence may include, but are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or	Examples of evidence may include, but are not limited to:

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column according to the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and 4.1.3 The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and CISA, or their successors.
4.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	After the Responsible Entity’s determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the Applicable Systems column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and CISA, or their successors.

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and CISA, or their successors.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible Entity's plan did not include one or more processes to provide notification per Requirement R4. (Part 1.2) OR The Responsible Entity's plan did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	The Responsible Entity did not develop a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible Entity's plan did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the Applicable Systems column for Part 1.2. (Part 1.2)
R2	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Par 2.1)	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity did not test the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column for Part 2.2 occurs. (Part 2.2)	retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the Applicable Systems column for Part 2.3. (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1) OR The Responsible Entity did not update the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity did not update the Cyber Security Incident response plan(s) or	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.1)

R #	**Violation Severity Levels (CIP-008-7)**			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
		The Responsible Entity did not update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	
R4	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3) OR The Responsible Entity did not report on one or more of the	The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the Applicable Systems column. (Requirement R4)	The Responsible Entity did not notify or update E-ISAC or CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity did not notify E-ISAC or CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	The Responsible Entity did not notify E-ISAC and CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Violation Severity Levels (CIP-008-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	attributes after determination pursuant to Part 4.1. (Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-008-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

Version	Date	Action	Change Tracking
7	TBD	Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed new or modified terms titled "Project 2016-02 CIP Definitions".

A. Introduction

1. **Title:** Cyber Security — Incident Reporting and Response Planning

2. **Number:** CIP-008-~~6~~7

3. **Purpose:** To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 **Balancing Authority**

4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the ~~BES:~~Bulk Electric System (BES):

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Remedial Action Scheme (RAS) where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 **Generator Operator**

4.1.4 **Generator Owner**

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each ~~Remedial Action Scheme~~RAS where the ~~Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers**: All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-008-~~6~~7:

4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP.

~~4.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems (BES) categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. ~~**5. Effective Dates:**~~

~~See Implementation Plan for CIP-008-6.~~

~~**6. Background:**~~

~~Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

"Applicable Systems~~" Columns in Tables:~~
": Each table has an "Applicable Systems" column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies.~~The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.~~

- ~~**High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~

~~**Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~

5. Effective Dates: See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~6~~7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-~~6~~7 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-~~6~~7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated~~:~~ Electronic Access Control and Monitoring Systems (EACMS) Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.
1.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1 That include criteria to evaluate and define attempts to compromise; 1.2.2 To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the ~~"~~“Applicable Systems~~"~~” column	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the ~~"~~“Applicable Systems~~"~~” column including justification for attempt determination criteria and documented processes for notification.

CIP-008-~~6~~7 Table R1 – Cyber Security Incident Response Plan Specifications

Part	Applicable Systems	Requirements	Measures
		for this Part; and 1.2.3 To provide notification per Requirement R4.	
1.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-~~6~~7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-~~6~~7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-~~6~~7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every~~-~~ 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the ~~“~~Applicable Systems~~”~~ column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

CIP-008-~~6~~7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing

Part	Applicable Systems	Requirements	Measures
2.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the “~~"~~Applicable Systems”~~"~~ column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the “~~"~~Applicable Systems”~~"~~ column.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-~~6~~7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-~~6~~7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

CIP-008-~~6~~7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, all of the following: 1. Dated documentation of~~-~~ post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or ~~•~~ Training sign-in sheets. •

~~CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication~~

~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
3.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the	~~An example~~Examples of evidence may include, but ~~is~~are not limited to: 1. Dated and revised Cyber Security Incident response plan with changes

CIP-008-~~6~~7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States ~~National~~ Cybersecurity ~~and Communications Integration Center (NCCIC),[1]~~ & Infrastructure Security Agency (CISA), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the ~~"~~Applicable Systems~~"~~ column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-~~6~~7 Table R4 – Notifications and Reporting for Cyber Security Incidents*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the ~~"~~Applicable Systems~~"~~ column according to the applicable requirement parts in *CIP-008-~~6~~7 Table R4 – Notifications and Reporting for Cyber Security Incidents.*

CIP-008-~~6~~7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1 The functional impact; 4.1.2 The attack vector used; and ~~4.1.3~~ The level of intrusion that was achieved or attempted. 4.1.3	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and ~~NCCIC.~~ CISA, or their successors.
4.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines:	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ~~NCCIC.~~ CISA, or their successors.

~~[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).~~

CIP-008-~~6~~7 Table R4 – Notifications and Reporting for Cyber Security Incidents

Part	Applicable Systems	Requirements	Measures
	Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	• One hour after the determination of a Reportable Cyber Security Incident. ~~•~~By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the “Applicable Systems” column for this Part. •	
4.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated~~:~~ EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within ~~7~~seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and ~~NCCIC.~~CISA, or their successors.

C. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~
- ~~Complaint~~

~~**1.4. Additional Compliance Information:**~~

~~None~~

~~2. Table of Compliance Elements~~

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-008-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~did not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (Part 1.3) OR The Responsible Entity ~~has developed the Cyber Security Incident response plan(s), but the plan does~~did not include incident handling procedures for Cyber Security Incidents. (Part 1.4) OR The Responsible ~~Entity has developed a Cyber Security Incident response plan, but the plan does~~Entity's plan did not include one or more processes to provide notification per Requirement R4. (Part 1.2) OR The Responsible ~~Entity has developed a Cyber Security Incident response plan, but~~	The Responsible Entity ~~has~~did not ~~developed~~develop a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (Part 1.1) OR The Responsible ~~Entity has developed a Cyber Security Incident response~~Entity's plan~~, but the plan does~~ did not include one or more processes to identify Reportable Cyber Security Incidents or a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Part 1.2.1, a system identified in the ~~“~~Applicable Systems~~”~~ column for Part 1.2. (Part 1.2)

R #	Violation Severity Levels (CIP-008-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~the plan does~~Entity’s plan did not include one or more processes that include criteria to evaluate and define attempts to compromise. (Part 1.2)	
R2	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Par 2.1)	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan(s). (Part 2.1)	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.2 occurs. (Part 2.2)	The Responsible Entity ~~has~~did not ~~tested~~test the Cyber Security Incident response plan(s) within 18 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents or Cyber Security Incidents that were an attempt to compromise a system identified in the “Applicable Systems” column for Part 2.3. (Part 2.3)
R3	The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120	The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a	The Responsible Entity ~~has~~ neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response

R #	Violation Severity Levels (CIP-008-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3)	to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.3) OR The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or	Reportable Cyber Security Incident. (Part 3.1.1) OR The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (Part 3.1.2) OR The Responsible Entity ~~has~~did not ~~updated~~update the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes. (Part 3.2)	to a Reportable Cyber Security Incident. (Part 3.1.1)

R #	Violation Severity Levels (CIP-008-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		• Technology changes. (Part 3.2)		
R4	The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.2 but failed to~~did not notify or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR ~~The Responsible Entity notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.3 but failed to~~The Responsible Entity did not report on one or more of the attributes within 7 days after determination of the attribute(s) not reported pursuant to Part 4.1. (Part 4.3)	The Responsible Entity ~~failed to~~did not notify E-ISAC or ~~NCCIC~~CISA, or their successors, of a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the ~~“~~Applicable Systems~~”~~ column. (Requirement R4)	The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident but failed to~~did not notify or update E-ISAC or ~~NCCIC~~CISA, or their successors, within the timelines pursuant to Part 4.2. (Part 4.2) OR The Responsible Entity ~~failed to~~did not notify E-ISAC or ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)	The Responsible Entity ~~failed to~~did not notify E-ISAC and ~~NCCIC~~CISA, or their successors, of a Reportable Cyber Security Incident. (Requirement R4)

R #	Violation Severity Levels (CIP-008-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity ~~notified E-ISAC and NCCIC, or their successors, of a Reportable Cyber Security Incident or a Cyber Security Incident that was an attempt to compromise a system identified in the “Applicable Systems” column for Part 4.1 but failed to~~did not report on one or more of the attributes after determination pursuant to Part 4.1. (Part 4.1)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-008-7 Technical Rationale

~~None.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change “Control Center” to “control center.”	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-008-5.	
5	7/9/14	FERC Letter Order issued approving VRFs and VSLs revisions to certain CIP standards.	CIP-008-5 Requirement R2, VSL table under Severe, changed from 19 to 18 calendar months.
6	2/7/2019	Adopted by the NERC Board of Trustees.	Modified to address directives in FERC Order No. 848

7	TBD	Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 CIP Definitions”.

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES).

4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1 Balancing Authority

    4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3 Generator Operator

    4.1.4 Generator Owner

4.1.5 Reliability Coordinator

4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-7:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*.

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	Examples of evidence may include, but are not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover Applicable System functionality.

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Examples of evidence may include, but are not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Examples of evidence may include, but are not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: - By recovering from an actual incident; - With a paper drill or tabletop exercise; or - With an operational exercise.	Examples of evidence may include, but are not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover Applicable System functionality substitutes for this test.	Examples of evidence may include, but are not limited to, operational logs or test results with criteria for testing the usability (e.g., sample tape load, browsing tape contents) and compatibility with current system configurations (e.g., manual, or automated comparison checkpoints between backup media contents and current configuration).
2.3	High impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the	Examples of evidence may include, but are not limited to, dated documentation of: - An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
		production environment. An actual recovery response may substitute for an operational exercise.	in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable Requirement Parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the Applicable Requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a	Examples of evidence may include, but are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS	defined role in the recovery plan of the updates.	including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information: None

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible Entity's plan(s) did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity plan(s) did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity did not create recovery plan(s) for Applicable Systems. OR The Responsible Entity plan(s) did not address the conditions for activation in Part 1.1. OR The Responsible Entity plan(s) did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan(s). (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 15 calendar months, not exceeding 16	The Responsible Entity did not test the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Part 2.2)	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 17 calendar months, not exceeding 18	The Responsible Entity did not test the recovery plan(s) according to Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR The Responsible Entity did not test a representative sample of the information used in the recovery of Applicable System functionality according to Part 2.2 within 18 calendar months between tests. (Part 2.2) OR

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)	OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)	calendar months between tests. (Part 2.2) OR The Responsible Entity did not test the recovery plan according to Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)	The Responsible Entity did not test the recovery plan(s) according to Part 2.3 within 39 calendar months between tests of the plan(s). (Part 2.3)
R3	The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar days of the update being completed. (Part 3.1.3)	The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity did not notify each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3) OR The Responsible Entity did not update the recovery plan(s) or notified each person or group with a defined role within 60	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1) OR The Responsible Entity did not update the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity did not update the recovery plan(s) or notified each person or group with a defined role within 90	The Responsible Entity neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.1)

R #	Violation Severity Levels (CIP-009-7)			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
		and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part 3.2)	calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-009-7 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See Separate document containing all proposed or modified terms titled “Project 2016-02 CIP Definitions”.

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for BES Cyber Systems

2. **Number:** CIP-009-~~6~~7

3. **Purpose:** To recover reliability functions performed by BES Cyber Systems (BCS) by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the Bulk Electric System (BES~~.~~).

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 **Balancing Authority**

4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each ~~Special Protection System or~~ Remedial Action Scheme (RAS) where the ~~Special Protection System or Remedial Action Scheme~~RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 **Generator Operator**

4.1.4 Generator Owner

~~**4.1.5 Interchange Coordinator or Interchange Authority**~~

~~4.1.6~~4.1.5 Reliability Coordinator

~~4.1.7~~4.1.6 Transmission Operator

~~4.1.8~~4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 ~~Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme~~Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-~~6~~7:

4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~**4.2.3.3**~~**4.2.3.4** The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~**4.2.3.4**~~**4.2.3.5** For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.3.5**~~**4.2.3.6** Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5.1 identification and categorization processes.

~~5. Effective Dates:~~

~~See Implementation Plan for CIP-009-6.~~

~~6. Background:~~

~~Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident~~

~~response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization’s overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~” Columns in Tables:~~

~~**5.1.**~~**4.3.** **”:** Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies.~~ The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.~~

- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.~~

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan”.

- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning]*.

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7 Table R1 – Recovery Plan Specifications*.

CIP-009-~~6~~7 Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-~~6~~7 Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover ~~BES Cyber~~Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover ~~BES Cyber~~Applicable System functionality.
1.4	High ~~I~~impact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium ~~I~~impact ~~BES Cyber Systems~~BCS at Control Centers and their associated: 1. EACMS; and PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Examples ~~An example~~ of evidence may include, but are not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High i~~I~~mpact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS Medium i~~I~~mpact ~~BES Cyber Systems~~BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this part	One or more processes to preserve data, per system ~~Cyber Asset~~ capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Examples ~~An example~~ of evidence may include, but are not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-~~6~~7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: - By recovering from an actual incident; - With a paper drill or tabletop exercise; or - With an operational exercise.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.
2.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and	Test a representative sample of information used to recover ~~BES Cyber~~Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover ~~BES Cyber~~Applicable System functionality substitutes for this test.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, operational logs or test results with criteria for testing the usability (e.g.~~.~~, sample tape load, browsing tape contents) and compatibility with current system configurations (e.g.~~.~~, manual, or automated comparison checkpoints between backup media contents and current configuration).

CIP-009-~~6~~7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
	~~2.~~ PACS ~~3.~~2.		
2.3	High ~~Impact BES Cyber Systems~~impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable ~~requirement parts~~Requirement Parts in *CIP-009-~~6~~7 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment]*.

M3. Acceptable evidence includes, but is not limited to, each of the ~~applicable requirement~~Applicable Requirement parts in *CIP-009-~~6~~7 Table R3 – Recovery Plan Review, Update and Communication*.

CIP-009-~~6~~7 Table R3 – Recovery Plan Review, Update and Communication

Part	Applicable Systems	Requirements	Measures
3.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
3.2	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact ~~-~~the ability to execute the recovery plan:	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or

CIP-009-~~6~~7 Table R3 – Recovery Plan Review, Update and Communication

Part	Applicable Systems	Requirements	Measures
	Medium ~~Impact BES Cyber Systems~~impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:
As defined in the NERC Rules of Procedure, “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

1.2. Evidence Retention:
The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Investigations
- Self-Reporting
- Complaints

1.4. Additional Compliance Information: None

Violation Severity Levels

R #	Violation Severity Levels (CIP-009-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	The Responsible ~~Entity has developed recovery~~Entity's plan(s~~), but the plan(s) do~~) did not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity ~~has developed recovery~~ plan(s~~), but the plan(s) do~~) did not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity ~~has~~did not ~~created~~create recovery plan(s) for ~~BES Cyber~~Applicable Systems. OR The Responsible Entity ~~has created recovery~~ plan(s) ~~for BES Cyber Systems, but the plan(s) does~~did not address the conditions for activation in Part 1.1. OR The Responsible Entity ~~has created recovery plan(s) for BES Cyber Systems, but the plan(s) does~~plan(s) did not address three or more of the requirements in Parts 1.2 through 1.5.
R2	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.1 within 15 calendar months, not exceeding 16 calendar months between	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (Part 2.1) OR	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (Part 2.1)	The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.1 within 18 calendar months between tests of the plan. (Part 2.1) OR

R #	Violation Severity Levels (CIP-009-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	tests of the plan~~. (~~(s). (Part 2.1) OR The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan according to ~~R2~~ Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests. (Part 2.3)	The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan according to ~~R2~~ Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests. (Part 2.3)	OR The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan according to ~~R2~~ Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests. (Part 2.3)	The Responsible Entity ~~has~~did not ~~tested~~test a representative sample of the information used in the recovery of ~~BES Cyber~~Applicable System functionality according to ~~R2~~ Part 2.2 within 18 calendar months between tests. (Part 2.2) OR The Responsible Entity ~~has~~did not ~~tested~~test the recovery plan(s) according to ~~R2~~ Part 2.3 within 39 calendar months between tests of the plan~~. (~~(s). (Part 2.3)
R3	The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 120 calendar	The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) based on any documented lessons learned within 90 and less than 120 calendar days of each recovery	The Responsible Entity~~ has~~ neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days -of each	The Responsible Entity~~ has~~ neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of each recovery plan

R #	Violation Severity Levels (CIP-009-~~6~~7)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	days of the update being completed. (Part 3.1.3)	plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity ~~has~~did not ~~notified~~notify each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (Part 3.1.3) OR The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or ~~–~~responsibilities, or • Responders, or • Technology changes. (Part 3.2)	recovery plan test or actual recovery. (Part 3.1.1) OR The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (Part 3.1.2) OR The Responsible Entity ~~has~~did not ~~updated~~update the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: ~~(3.2)~~ • Roles or responsibilities, or • Responders, or • Technology changes. (Part (3.2)	test or actual recovery. (Part 3.1.1)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-009-7 Technical Rationale

~~None.~~

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-009-5.	
6	11/13/14	Adopted by the NERC Board of Trustees.	Addressed FERC directives from Order No. 791
6	1/21/16	FERC Order issued approving CIP-009-6. Docket No. RM15-14-000	
7	TBD	Virtualization Modifications	

~~Guidelines and Technical Basis~~

~~Section 4 – Scope of Applicability of the CIP Cyber Security Standards~~

~~Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.~~

~~Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.~~

~~Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.~~

~~Requirement R1:~~

~~The following guidelines are available to assist in addressing the required components of a recovery plan:~~

- ~~NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf~~
- ~~National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf~~

~~The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.~~

~~A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.~~

~~For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.~~

~~For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.~~

~~For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:~~

1. ~~Installation files and media;~~
2. ~~Current backup tapes and any additional documented configuration settings;~~
3. ~~Documented build or restoration procedures; and~~
4. ~~Cross site replication storage.~~

~~For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:~~

- ~~Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.~~
- ~~Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.~~
- ~~Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.~~
- ~~Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.~~

~~The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.~~

~~For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.~~

~~**Requirement R2:**~~

~~A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.~~

~~A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.~~

~~Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."~~

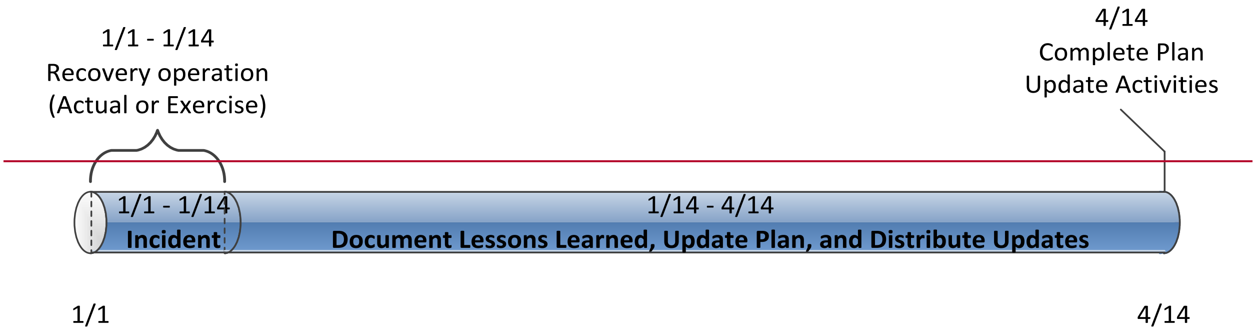
~~The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."~~

~~For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.~~

~~Requirement R3:~~

~~This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.~~

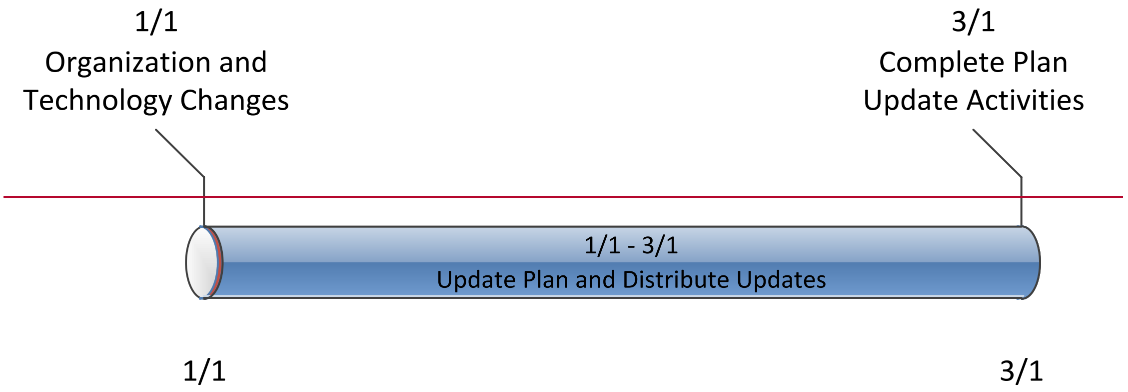
~~The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.~~



~~**Figure 1: CIP-009-6 R3 Timeline**~~

~~The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.~~

~~The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.~~



~~**Figure 2: Timeline for Plan Changes in 3.2**~~

~~When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.~~

~~Rationale:~~

~~During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.~~

~~Rationale for Requirement R1:~~

~~Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.~~

~~Rationale for Requirement R2:~~

~~The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.~~

~~Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.~~

~~Rationale for Requirement R3:~~

~~To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.~~

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29, 2023

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed or modified terms titled “Project 2016-02 CIP Definitions”.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-5

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-5:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and

data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Date:** See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.	Examples of evidence may include, but are not limited to, one or more documented process(es) that authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity, such as: • Change records documenting the authorization. • Change records authorizing systems to automate changes to Applicable Systems. Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) • Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) • Configuration of malicious code prevention methods (CIP-007 R3) • Configuration of security event logging/alerting (CIP-007 R4) • Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5) • Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)
1.2	High impact BCS	1.2.1. Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, to ensure that required cyber security controls in CIP-005 and CIP-007 are not	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test, or logs from systems that automatically remediate deviations in required cyber security controls in CIP-005 and CIP-007.

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
		adversely affected; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.
1.4	High impact BCS and their associated: 1. EACMS;	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the	An example of evidence may include, but is not limited to:

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	altered cyber security controls were not adversely affected.	• System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods;	An example of evidence may include, but is not limited to, documented methods to monitor at least once every 35 calendar days. Monitoring system configuration or procedural controls demonstrating monitoring of at least one cyber security control for 2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
		2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements or additions with a previously assessed configuration of an existing Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of tools used to perform the assessment; or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of evidence may include, but are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA, and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.		The Responsible Entity's change management process(es) does not include one of the required items listed in 1.2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.3.1 through 1.3.2. (Part 1.3)	The Responsible Entity change management process(es) did not include authorization for changes as required in Part 1.1. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.2.1 through 1.2.2. (Part 1.2); OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) OR The Responsible Entity's change management process(es) does not include verification, as required by Part 1.4. (Part 1.4)	The Responsible Entity neither documented nor implemented any change management process(es) that include required items in Part 1.1 through Part 1.4. (Requirement R1)
R2.	The Responsible Entity did not monitor within 35 calendar days, but less than 70 calendar days as required by Part 2.1.	The Responsible Entity's documented and implemented configuration monitoring process(es) does not include one or two of the required	The Responsible Entity's documented and implemented configuration monitoring process(es) does not include three or four of the required	The Responsible Entity neither documented nor implemented a configuration monitoring process(es); or the process does not include five or more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 70 calendar days, but less than 105 calendar days as required by Part 2.1.	Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 105 calendar days, but less than 140 calendar days as required by Part 2.1.	of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 140 calendar days or more as required by Part 2.1. OR The Responsible Entity neither documented nor investigated detected unauthorized changes. (Part 2.1)
R3.	The Responsible Entity performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its Applicable Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its Applicable Systems. (Part 3.2)	The Responsible Entity did not implement any vulnerability assessment processes for one of its Applicable Systems. (Requirement R3) OR The Responsible Entity performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity performed an active vulnerability assessment more

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				than 45 months since the last active assessment on one of its applicable BES Cyber Systems. (Part 3.2) OR The Responsible Entity did not perform the active vulnerability assessment of a Cyber System prior to it becoming an Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (Part 3.4)
R4.	The Responsible Entity did not manage its Transient Cyber Asset(s) according to Attachment 1, Section 1.1. (Requirement R4)	The Responsible Entity did not implement the Removable Media sections according to Attachment 1, Section 3. (Requirement R4)	The Responsible Entity did not authorize its TCA(s) according to Attachment 1, Section 1.2. (R4)	The Responsible Entity did not document or implement one or more plan(s) for TCAs and Removable Media according to

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	OR The Responsible Entity did not document the Removable Media sections according to Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity did not document authorization for TCA managed by the Responsible Entity according to Attachment 1, Section 1.2. (Requirement R4)	OR The Responsible Entity did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCA managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	OR The Responsible Entity did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for TCAs managed by the Responsible Entity according to Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR The Responsible Entity did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for TCAs managed by a party other than the Responsible Entity according to Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	Requirement R4. (Requirement R4)

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-010-5 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	
4	3/18/2021	FERC order approving Docket No. RD21-2-000	
4	4/5/2021	Effective Date	10/1/2022
5	TBD	Virtualization Modifications	

Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Live operating system and software executable only from read only media;
- System hardening; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read only media;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

2.3. For any method used as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting ; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCA(s). This can be included as part of the TCA(s), part of the documentation related to authorization of TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating system and software executable only from read only media, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the risk of software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, methods to maintain the known good state of the OS and all software, or system hardening practices. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail,

policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that that document a review of the use of live operating system and software executable only from read only media; memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that that document a review of the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, and system hardening by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with initial ballot	January 21 - March 22, 2021
63-day formal comment period with additional ballot	June 30 - September 1, 2021
53-day formal comment period with additional ballot	February 18 - April 12, 2022
45-day formal comment period with additional ballot	August 17 - October 3, 2022
45-day formal comment period with additional ballot	October 3 - November 29, 2023

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed or modified terms titled “Project 2016-02 CIP Definitions”.

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

~~1.~~2. Number: CIP-010-~~4~~5

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems (BCS) by specifying configuration change management and vulnerability assessment requirements in support of protecting ~~BES Cyber Systems~~BCS from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

~~2.~~4. Applicability:

~~2.1.~~4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

~~2.2.~~4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in Section 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-~~4~~5:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

~~**3. Effective Date:** See Implementation Plan for Project 2019-03.~~

~~**4. Background:** Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the~~

~~standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~” Columns in Tables:~~

4.3. ”: Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies. ~~The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.~~

- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~
- ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

5. Effective Date: See “Project 2016-02 Modifications to CIP Standards Implementation Plan.”

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) to manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-~~4~~5 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~4~~5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~4~~5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
~~**1.1**~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2.1. PACS; and~~ ~~3.1. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~Develop a baseline configuration, individually or by group, which shall include the following items:~~ ~~1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;~~ ~~1.1.2. Any commercially available or open-source application software (including version) intentionally installed;~~ ~~1.1.3. Any custom software installed;~~ ~~1.1.4. Any logical network accessible ports; and~~ ~~1.1.5. Any security patches applied.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or~~ ~~• A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.~~
~~**1.2**~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~	~~Authorize and document changes that deviate from the existing baseline configuration.~~	~~Examples of evidence may include, but are not limited to:~~ ~~• A change request record and~~

CIP-010-~~4~~5 Table R1 – Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~		~~associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or~~ ~~• Documentation that the change was performed in accordance with the requirement.~~
~~1.3~~	~~High Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~ ~~Medium Impact BES Cyber Systems and their associated:~~ ~~1. EACMS;~~ ~~2. PACS; and~~ ~~3. PCA~~	~~For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.~~	~~An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.~~
1.~~4~~1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); ~~1.~~ Physical Access Control~~EACMS;~~ ~~2.1.~~ ~~PACS; and~~ ~~3.1.~~ ~~PCA~~ 2. ~~Medium Impact BES Cyber~~ Systems (PACS); and	~~For a change~~Authorize changes that ~~deviates from~~affect Applicable Systems where those changes alter the ~~existing baseline configuration:~~ ~~1.4.1. Prior to the change, determine required~~behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 ~~and~~or CIP-007 ~~that~~	~~An example~~Examples of evidence may include, but ~~is~~are not limited to, ~~a list~~one or more documented process(es) that authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls ~~verified or tested along with the dated test results.~~, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity, such as:

CIP-010-~~4~~5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: ~~4.~~1. EACMS; ~~5.~~2. PACS; and ~~6.~~3. PCA SCI supporting an Applicable System in this Part.	~~could be impacted~~, as defined by the ~~change;~~ ~~1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and~~ ~~Document the results of the verification~~Responsible Entity.	• Change records documenting the authorization. • Change records authorizing systems to automate changes to Applicable Systems. Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) • Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) • Configuration of malicious code prevention methods (CIP-007 R3) • Configuration of security event logging/alerting (CIP-007 R4) • Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5)

CIP-010-~~4~~5 Table R1 – ~~-~~Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
			• Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)
1.~~5~~2	High ~~Impact BES Cyber Systems~~impact BCS	~~Where technically feasible, for each change that deviates from the existing baseline configuration:~~ 1.2.1. Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, ~~that models the baseline configuration~~ to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test~~.~~ , or logs from systems that automatically remediate deviations in required cyber security controls in CIP-005 and CIP-007.
1.~~6~~3	High ~~Impact BES Cyber Systems~~impact	Prior to ~~a change that deviates from~~ the	An example of evidence may include, but is

CIP-010-~~4~~5 Table R1 – ~~-~~Configuration Change Management

Part	Applicable Systems	Requirements	Measures
	BCS and their associated: 1. EACMS; and 2. PACS Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	~~existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5,~~installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.~~6~~3.1.~~–~~ Verify the identity of the software source; and 1.~~6~~3.2.~~–~~ Verify the integrity of the software obtained from the software source.	not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to ~~the baseline change~~installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.
1.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the altered cyber security controls were not adversely affected.	An example of evidence may include, but is not limited to: • System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

CIP-010-45 Table R1 – -Configuration Change Management

Part	Applicable Systems	Requirements	Measures

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-~~4~~5 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~4~~5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~4~~5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact~~impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	~~Monitor~~Methods to monitor, per system capability, at least once every 35 calendar days, for ~~changes to~~ unauthorized changes that affect Applicable Systems, where those changes alter the ~~baseline configuration (as described~~behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in ~~Requirement R1, Part~~ CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1~~).~~. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches.	An example of evidence may include, but is not limited to, ~~logs from a~~documented methods to monitor at least once every 35 calendar days. Monitoring system ~~that is monitoring the~~ configuration or procedural controls demonstrating monitoring of at least one cyber security control for 2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

CIP-010-45 Table R2 – Configuration Monitoring

Part	Applicable Systems	Requirements	Measures
		2.1.4. Configuration of malicious code protection methods; 2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~3~~5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~3~~5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-45 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High ~~Impact~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact~~impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every -15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-45 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.2	High ~~Impact~~impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	~~Where technically feasible, at~~At least once every 36 calendar months, per system capability: ~~2.2.1~~3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects~~, that models the baseline configuration of the BES Cyber System in a production environment~~; and ~~2.2.2~~3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-45 Table R3 – Vulnerability Assessments

Part	Applicable Systems	Requirements	Measures
3.3	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Prior to ~~adding~~becoming a new ~~applicable Cyber Asset to a production environment~~Applicable System, perform an active vulnerability assessment of the new ~~Cyber Asset~~Applicable System, except for ~~CIP Exceptional Circumstances and like~~: • Like replacements ~~of the same type of Cyber Asset~~or additions with a ~~baseline~~previously assessed configuration ~~that models~~of an existing ~~baseline configuration of the previous or other existing Cyber Asset.~~Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to~~, a document listing~~: • The output of tools used to perform the assessment; or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment ~~(~~performed prior to ~~the commissioning of the~~ becoming a new ~~Cyber Asset) and the output of any tools used to perform the assessment.~~ Applicable System.

CIP-010-~~4~~5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	~~An example~~Examples of evidence may include, but ~~is~~are not limited to~~, a document~~: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA, and associated ~~Protected Cyber Assets~~SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for ~~Transient Cyber Assets~~TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for ~~Transient Cyber Assets~~TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use ~~Transient Cyber Asset~~TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use ~~Transient Cyber Asset~~TCA(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: “Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	~~The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)~~	The Responsible ~~Entity has documented and implemented a configuration~~Entity's change management process(es) ~~that includes only three~~does not include one of the required ~~baseline~~ items listed in 1.~~1~~2.1 through 1.2.2. (Requirement R1 Part 1.2); OR The Responsible Entity's change management process(es) does not include one of the required items listed in 1.~~5. (~~3.1~~.~~ through 1.3.2. (Part 1.3)	The Responsible Entity ~~has documented and implemented a configuration~~ change management process(es) ~~that includes only two of the~~ did not include authorization for changes as required ~~baseline~~in Part 1.1. (Part 1.1) OR The Responsible Entity's change management process(es) does not include the two required items listed in 1.~~1~~2.1 through 1.2.2. (Part 1.~~5. (1.1)~~2); OR The Responsible ~~Entity has a~~Entity's change management process ~~as specified in Part 1.6 to verify the identity of the software source (1.6.1) but~~(es) does not include the two required items listed in 1.3.1 through 1.3.2. (Part 1.3) OR ~~have a~~The Responsible Entity's change management process ~~as specified in~~ (es)	The Responsible Entity ~~has not~~neither documented ~~or~~nor implemented any ~~configuration change management process(es). (R1)~~ ~~OR~~ ~~The Responsible Entity has documented and implemented a configuration~~ change management process(es) that ~~includes only one of the~~include required ~~baseline~~ items ~~listed~~ in Part 1.~~1.~~1 through ~~1.1.5. (1.1)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2~~Part ~~)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) to~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			does not include verification, as required by Part 1.~~6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source.~~ ~~(1.6.2~~4. (Part 1.4)	~~update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3)~~ ~~OR~~ ~~The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (~~1.4.~~1~~ (Requirement R1) ~~OR~~ ~~The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~following the change. (1.4.2 & 1.4.3)~~ ~~OR~~ ~~The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1)~~ ~~OR~~ ~~The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)~~ ~~OR~~ ~~The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by~~

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)~~
R2.	~~N/A~~The Responsible Entity did not monitor within 35 calendar days, but less than 70 calendar days as required by Part 2.1.	~~N/A~~The Responsible Entity's documented and implemented configuration monitoring process(es) does not include one or two of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 70 calendar days, but less than 105 calendar days as required by Part 2.1.	~~N/A~~The Responsible Entity's documented and implemented configuration monitoring process(es) does not include three or four of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor within 105 calendar days, but less than 140 calendar days as required by Part 2.1.	The Responsible Entity ~~has not~~neither documented ~~or~~nor implemented a configuration monitoring process(es~~) to~~); or the process does not include five or more of the required Parts 2.1.1 through 2.1.7 for Applicable Systems as required in Part 2.1. OR The Responsible Entity did not monitor ~~for, investigate, and document~~within 140 calendar days or more as required by Part 2.1. OR The Responsible Entity neither documented nor investigated detected unauthorized changes~~ to the baseline at least once every 35 calendar days. (~~. (Part 2.1)
R3.	The Responsible Entity~~ has implemented one or more documented vulnerability~~	The Responsible Entity~~ has implemented one or more documented vulnerability~~	The Responsible Entity~~ has implemented one or more documented vulnerability~~	The Responsible Entity ~~has~~did not ~~implemented~~implement any vulnerability assessment

R #	Violation Severity Levels			
	Lower VSL	**Moderate VSL**	**High VSL**	**Severe VSL**
	~~assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.1) OR The Responsible Entity~~ has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.2)	~~assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 18 months, but less than 21 months, since the last assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.1) OR The Responsible Entity~~ has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.2)	~~assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.1) OR The Responsible Entity~~ has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its ~~applicable BES Cyber~~Applicable Systems. (Part 3.2)	processes for one of its ~~applicable BES Cyber~~Applicable Systems. (Requirement R3) OR The Responsible Entity~~ has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has~~ performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (Part 3.1) OR The Responsible Entity~~ has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has~~ performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems~~.(~~. (Part 3.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity ~~has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but~~ did not perform the active vulnerability assessment ~~in~~of a ~~manner that models~~Cyber System prior to it becoming an ~~existing baseline configuration of its applicable BES Cyber~~Applicable Systems. (Part 3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its ~~applicable BES Cyber~~Applicable Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				plan, and the execution status of the mitigation plans. (Part 3.4)
R4.	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not manage its Transient Cyber Asset(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.1. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document the Removable Media sections according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document authorization for ~~Transient~~	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement the Removable Media sections according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 3. (Requirement R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to~~did not document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not authorize its ~~Transient Cyber Asset~~TCA(s) according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (R4) OR The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for ~~Transient Cyber Assets~~TCAs managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 1.3, 1.4, and 1.5. (Requirement R4) OR	The Responsible Entity ~~failed to~~did not document or implement one or more plan(s) for ~~Transient Cyber Assets~~TCAs and Removable Media according to ~~CIP-010-4,~~ Requirement R4. (Requirement R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	~~Cyber Assets~~TCA managed by the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Section 1.2. (Requirement R4)	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	The Responsible Entity ~~documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to~~did not implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for ~~Transient Cyber Assets~~TCAs managed by a party other than the Responsible Entity according to ~~CIP-010-4, Requirement R4,~~ Attachment 1, Sections 2.1, 2.2, and 2.3. (Requirement R4)	

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan~~ for Project 2019-03.~~”.
- CIP-010-45 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	
3	10/18/2018	FERC Order approving CIP-010-3. -Docket No. RM17-13-000.	
4	08/01/2019	Modified to address directives in FERC Order No. 850.	Revised
4	11/05/2020	Adopted by the NERC Board of Trustees.	
4	3/18/2021	FERC order approving Docket No. RD21-2-000	
4	4/5/2021	Effective Date	10/1/2022
5	TBD	Virtualization Modifications	

Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

Section 1. ~~Transient Cyber Asset~~TCA(s) Managed by the Responsible Entity.

1.1. ~~Transient Cyber Asset~~TCA Management: Responsible Entities shall manage ~~Transient Cyber Asset~~TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection ~~to a BES Cyber System~~, or (3) a combination of both (1) and (2) above.

1.2. ~~Transient Cyber Asset~~TCA Authorization: For each individual or group of ~~Transient Cyber Asset~~TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset (per Transient Cyber Asset~~TCA (per TCA capability):

- Security patching, including manual or managed updates;
- ~~Live operating system and software executable only from read-only media;~~
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; ~~or~~
- Live operating system and software executable only from read only media;
- System hardening; or

- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of ~~Transient Cyber Asset~~TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 2. ~~Transient Cyber Asset~~TCA(s) Managed by a Party Other than the Responsible Entity.

2.1. Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the ~~Transient Cyber Asset (per Transient Cyber Asset~~TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- ~~Other~~Review of other method(s) to mitigate software vulnerabilities.

2.2. Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per ~~Transient Cyber Asset~~TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read~~-~~ only media;
- Review of system hardening used by the party; or
- ~~Other~~Review of other method(s) to mitigate the risk of introduction of malicious code.

2.3. For any method used ~~to mitigate software vulnerabilities or malicious code~~ as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the ~~Transient Cyber Asset~~TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

- **3.1.1.** Users, either individually or by group or role; and
- **3.1.2.** Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code~~ to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets~~, each Responsible Entity shall:

- **3.2.1.** Use method(s) to detect malicious code on Removable Media ~~using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets~~prior to connecting ; and
- **3.2.2.** Mitigate the threat of detected malicious code~~ on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets~~.

CIP-010-~~4~~5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the ~~Transient Cyber Asset~~TCA(s). This can be included as part of the ~~Transient Cyber Asset plan~~TCA(s), part of the documentation related to authorization of ~~Transient Cyber Asset~~TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of ~~Transient Cyber Asset~~TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating ~~systems~~ system and software executable only from read~~-~~only media, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the risk of software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, methods to maintain the known good state of the OS and all software, or ~~procedures or processes associated with~~ system hardening practices. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that that document a review of the use of live operating system and software executable only from read only media; memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that that document a review of the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, ~~use of live of operating systems or~~and system hardening ~~performed~~ by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for ~~Transient Cyber Asset~~TCA(s) managed by a party other than the Responsible Entity. If a ~~Transient Cyber Asset~~TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the ~~Transient Cyber Asset~~TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the ~~Transient Cyber Asset~~TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
45-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed or modified terms titled “Project 2016-02 CIP Definitions”

A. Introduction

1. **Title:** Cyber Security — Information Protection
2. **Number:** CIP-011-4
3. **Purpose:** To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
4. **Applicability:**

    4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

    4.1.1 Balancing Authority

    4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

    4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

    4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

    4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

    4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

    4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

    4.1.3 Generator Operator

    4.1.4 Generator Owner

    4.1.5 Reliability Coordinator

    4.1.6 Transmission Operator

4.1.7 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:
All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-4:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002 identification and categorization processes.

4.3. **“Applicable Systems”:** Each table has an “Applicable Systems” column to define the scope of systems to which a specific requirement part applies.

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards” Implementation Plan.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BCSI pertaining to Applicable Systems identified in *CIP-011-4 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include

CIP-011-4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
	1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part		topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-4 Table R2 –Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4 Table R2 –Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-4 Table R2 –Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).	Examples of evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

B. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-011-4)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity did not implement one or more BCSI protection program(s). (Requirement R1) OR The Responsible Entity did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity did not include processes for reuse to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity did not include disposal processes to prevent the unauthorized retrieval of BCSI from an Applicable System. (Part 2.1)	The Responsible Entity neither documented nor implemented any processes for applicable requirement parts in CIP-011-4 Table R2 –Reuse and Disposal. (Requirement R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-011-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
3	12/7/21	FERC Order issued approving CIP-011-3 Docket No. RD21-6-000	“A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability

Version	Date	Action	Change Tracking
			Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.”
3	12/10/21	Effective Date	1/1/2024
4	TBD	Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
45-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed or modified terms titled “Project 2016-02 CIP Definitions”

A. Introduction

1. **Title:** Cyber Security — Information Protection

2. **Number:**~~–~~ CIP-011-~~3~~4

3. **Purpose:**~~-~~ To prevent unauthorized access to BES Cyber System Information (BCSI) by specifying information protection requirements in support of protecting BES Cyber Systems (BCS) against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

~~3.~~4. **Applicability:**

~~3.1.~~4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

~~3.1.1~~4.1.1 **Balancing Authority**

~~3.1.2~~4.1.2 **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

~~3.1.2.1~~4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

~~3.1.2.1.1~~4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

~~3.1.2.1.2~~4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

~~3.1.2.2~~4.1.2.2 Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.1.2.3~~4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.1.2.4~~4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~3.1.3~~4.1.3 **Generator Operator**

~~3.1.4~~4.1.4 **Generator Owner**

~~3.1.5~~4.1.5 **Reliability Coordinator**

~~3.1.6~~4.1.6 **Transmission Operator**

~~3.1.7~~4.1.7 **Transmission Owner**

~~3.2.~~4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

~~3.2.1~~4.2.1 **Distribution Provider**: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

~~3.2.1.1~~4.2.1.1 Each UFLS or UVLS System that:

~~3.2.1.1.1~~4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

~~3.2.1.1.2~~4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

~~3.2.1.2~~4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.2.1.3~~4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.2.1.4~~4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~3.2.2~~4.2.2 **Responsible Entities listed in 4.1 other than Distribution Providers:** All BES Facilities.

~~3.2.3~~4.2.3 **Exemptions:** The following are exempt from Standard CIP-011-~~3~~4:

~~3.2.3.1~~4.2.3.1 Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

~~3.2.3.2~~4.2.3.2 Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters~~.~~ (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~3.2.3.3~~4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~3.2.3.4~~4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~3.2.3.5~~4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002~~-5.1a~~ identification and categorization processes.

~~1. **Effective Dates:** See Implementation Plan for CIP-011-3.~~

~~2. **Background:** Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.~~

~~Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.~~

~~The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.~~

~~The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.~~

~~Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.~~

~~Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.~~

~~Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and~~

~~implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.~~

~~Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an “or,” and numbered items are items that are linked with an “and.”~~

~~Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.~~

“Applicable Systems~~***” Columns in Tables:***~~

~~3.3.~~**4.3. ”:** Each table has an “Applicable Systems” column to ~~further~~ define the scope of systems to which a specific requirement ~~row~~part applies.~~ The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.~~

- ~~**High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.~~
- ~~**Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.~~

5. **Effective Dates:** See “Project 2016-02 Modifications to CIP Standards” Implementation Plan.

- B. ~~**Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.~~
- ~~**Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.~~

Requirements and Measures

R1. ~~**R1.**~~ Each Responsible Entity shall implement one or more documented information protection program(s) for ~~BES Cyber System Information (~~BCSI~~)~~ pertaining to ~~"~~Applicable Systems~~"~~ identified in *CIP-011-~~3~~4 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-~~3~~4 Table R1 – Information Protection Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1.~~-~~ Evidence for the information protection program must include the applicable requirement parts in *CIP-011-~~3~~4 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~3~~4 Table R1 – Information Protection Program

Part	Applicable Systems	Requirements	Measures
1.1	High ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium ~~Impact BES Cyber Systems~~ impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of ~~acceptable~~ evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to identify BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.
1.2	High ~~I~~impact BCS and their associated:	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following:

CIP-011-~~3~~4 Table R1 – Information Protection Program

Part	Applicable Systems	Requirements	Measures
	1. EACMS; and 2. PACS Medium ~~I~~impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part		- Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or - Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: - Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or - Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or - Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-~~3~~4 Table R2 –~~ BES Cyber Asset ~~Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*.

M2.~~-~~ Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-~~3~~4 Table R2 –~~ BES Cyber Asset ~~Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-~~3~~4 Table R2 –~~BES Cyber Asset ~~Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium ~~Impact BES Cyber Systems~~impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	~~Prior to the release for~~Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse ~~of applicable Cyber Assets that contain BCSI ~~(except for reuse within other systems identified in the ~~“~~"Applicable Systems~~”~~" column~~), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.~~).	Examples of~~ acceptable~~ evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

B. Compliance

1. **Compliance Monitoring Process:**

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- The applicable entity shall retain evidence of each requirement in this standard for three calendar years.
- If an applicable entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels (CIP-011-~~3~~4)			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	N/A	N/A	The Responsible Entity ~~documented, but~~ did not~~,~~ implement one or more BCSI protection program(s). ~~(~~ (Requirement R1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to identify BCSI. (Part 1.1) OR The Responsible Entity ~~documented but~~ did not implement at least one method to protect and securely handle BCSI. (Part 1.2)	The Responsible Entity neither documented nor implemented one or more BCSI protection program(s). (Requirement R1)
R2	N/A	The Responsible Entity ~~implemented one or more~~ ~~documented~~did not include processes for reuse to prevent the unauthorized retrieval of BCSI from ~~the BES Cyber Asset~~an Applicable System. (Part 2.1)	The Responsible Entity ~~implemented one or more~~ ~~documented~~did not include disposal processes to prevent the unauthorized retrieval of BCSI from an Applicable System~~the BES Cyber Asset~~. (Part 2.1)	The Responsible Entity ~~has not~~neither documented ~~or~~ nor implemented any processes for applicable requirement parts in CIP-011-4 Table R2 –Reuse and Disposal. (Requirement R2)

C. Regional Variances

None.

D. Interpretations

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-011-4 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-011-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-011-2. Docket No. RM15-14-000	
3	8/12/21	Adopted by the NERC Board of Trustees	Revised to enhance BES reliability for entities to manage their BCSI.
3	12/7/21	FERC Order issued approving CIP-011-3 Docket No. RD21-6-000	"A Responsible Entity may elect to comply with the requirements in CIP-004-7 and CIP-011-3 following their approval by the applicable governmental authority, but prior to their Effective Date. In such a case, the Responsible Entity shall notify the applicable Regional Entities of the date of compliance with the CIP-004-7 and CIP-011-3 Reliability

Version	Date	Action	Change Tracking
			Standards. Responsible Entities must comply with CIP-004-6 and CIP-011-2 until that date.”
3	12/10/21	Effective Date	1/1/2024
4	TBD	Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed or modified terms titled "Project 2016-02 CIP Definitions"

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-3**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems (BCS).

4. **Applicability:**

4.1. **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. **Balancing Authority**

4.1.2. **Distribution Provider** that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.3. **Generator Operator**

4.1.4. **Generator Owner**

4.1.5. **Reliability Coordinator**

4.1.6. **Transmission Operator**

4.1.7. **Transmission Owner**

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in

this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider:** One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers:** All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-013-3:

4.2.3.1. Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. **Effective Date:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan".

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable systems listed in Requirement R1 to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring applicable systems listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity's supply chain cyber risk management plan(s) did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1. OR The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) in planning for procurement applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring applicable systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in Requirement R1.
R2.	The Responsible Entity did not implement one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity did not implement the use of process(es) for procuring applicable systems as specified in Part 1.2.	The Responsible Entity did not implement the use of process(es) in planning for procurement of applicable systems as specified in Part 1.1, and did not implement the use of process(es) for

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				procuring applicable systems as specified in Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in Requirement R2.
R3.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 16th calendar month since the previous review.	The Responsible Entity exceeded the 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 17th calendar month since the previous review.	The Responsible Entity exceeded 15 calendar months by reviewing and obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) in the 18th calendar month since the previous review.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review.

D. Regional Variances

None.

E. Associated Documents

- Implementation Plan for Project 2016-02
- CIP-013-3 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	
2	3/18/2021	FERC Order approving CIP-013-2. Docket No. RD21-2-000.	
2	4/5/2021	Effective Date	10/1/2022
3	TBD	Virtualization Modifications	

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

This is the final draft of the proposed standard.

Completed Actions	Date
Standards Committee (SC) approved Standard Authorization Request (SAR) for posting	March 9, 2016
SAR posted for comment	March 23 - April 21, 2016
SAR posted for comment	June 1 - 30, 2016
SC Accepted the SAR	July 20, 2016
60-day formal comment period with ballot	January 21 - March 22, 2021
63-day formal comment period with ballot	June 30 - September 1, 2021
53-day formal comment period with ballot	February 18 - April 12, 2022
45-day formal comment period with ballot	August 17 - September 30, 2022

Anticipated Actions	Date
Final Ballot	April 3 - 12, 2024
Board adoption	May 2024

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): See separate document containing all proposed or modified terms titled “Project 2016-02 CIP Definitions”

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-~~2~~3**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems~~.~~ (BCS).

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as “Responsible Entities.” For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

   4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in

this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. **Distribution Provider:** One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. **Responsible Entities listed in 4.1 other than Distribution Providers:** All BES Facilities.

4.2.3. **Exemptions:** The following are exempt from Standard CIP-013-~~2~~3:

4.2.3.1. Cyber ~~Assets~~Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber ~~Assets~~Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. Cyber Systems, associated with communication networks and data communication links, between Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

~~4.2.3.3.~~4.2.3.4. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

~~4.2.3.4.~~4.2.3.5. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.3.5.~~4.2.3.6. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002 or any subsequent version of that Reliability Standard.

5. **Effective Date:** See "Project 2016-02 Modifications to CIP Standards Implementation Plan~~ for Project 2019-03.~~".

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact ~~BES Cyber Systems~~BCS and their associated Electronic Access Control or Monitoring Systems (EACMS~~) and~~), Physical Access Control Systems (PACS), and Shared Cyber Infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of ~~BES Cyber Systems and their associated EACMS and PACS~~applicable systems listed in Requirement R1 to identify and assess cyber security risk(s) to the ~~Bulk Electric System~~BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring ~~BES Cyber Systems, and their associated EACMS and PACS,~~applicable systems listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor~~ for use in the BES Cyber System and their associated EACMS and PACS~~; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

“Compliance Enforcement Authority” (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, “Compliance Monitoring and Enforcement Program” refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible ~~Entity developed one or more documented~~Entity's supply chain cyber ~~security~~ risk management plan(s) ~~which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do~~did not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible ~~Entity developed one or more documented~~Entity's supply chain cyber security risk management plan(s) ~~which include the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Part 1.2, but the plans do~~did not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible ~~Entity developed one or more documented~~Entity's supply chain cyber security risk management plan(s~~), but the plan(s~~) did not include the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~applicable systems as specified in Part 1.1~~, or the~~. OR The Responsible Entity's supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~applicable systems as specified in Part 1.2.	The Responsible ~~Entity developed one or more documented~~Entity's supply chain cyber security risk management plan(s~~), but the plan(s~~) did not include the use of process(es) in planning for procurement ~~of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~applicable systems as specified in Part 1.1, and the supply chain cyber security risk management plan(s) did not include the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~applicable systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				cyber security risk management plan(s) as specified in ~~the~~ Requirement R1.
R2.	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but~~ did not implement one of the parts in ~~Requirement R1~~ Part 1.2.1 through Part 1.2.6.	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber Systems and their associated EACMS and PACS, as specified in Requirement R1 Part 1.2, but~~ did not implement two or more of the parts in ~~Requirement R1~~ Part 1.2.1 through Part 1.2.6.	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or~~ did not implement the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~applicable systems as specified in ~~Requirement R1~~ Part 1.2.	The Responsible Entity ~~implemented its supply chain cyber security risk management plan(s), but~~ did not implement the use of process(es) in planning for procurement of ~~BES Cyber Systems, and their associated EACMS and PACS, to identify and assess cyber security risk(s) to the BES~~applicable systems as specified in ~~Requirement R1~~ Part 1.1, and did not implement the use of process(es) for procuring ~~BES Cyber Systems and their associated EACMS and PACS,~~applicable systems as specified in ~~Requirement R1~~ Part 1.2; OR

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in ~~the requirement.~~Requirement R2.
R3.	The Responsible Entity ~~reviewed~~exceeded 15 calendar months by reviewing and ~~obtained~~obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than 15 calendar months but less than or equal to 16~~in the 16th calendar ~~months~~month since the previous review ~~as specified in the Requirement~~.	The Responsible Entity ~~reviewed~~exceeded the 15 calendar months by reviewing and ~~obtained~~obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than 16 calendar months but less than or equal to 17~~in the 17th calendar ~~months~~month since the previous review ~~as specified in the Requirement~~.	The Responsible Entity ~~reviewed~~exceeded 15 calendar months by reviewing and ~~obtained~~obtaining CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) ~~but did so more than 17 calendar months but less than or equal to 18~~in the 18th calendar ~~months~~month since the previous review ~~as specified in the Requirement~~.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review ~~as specified in the Requirement.~~.

D. Regional Variances

None.

E. Associated Documents

- See “Project 2016-02 Modifications to CIP Standards Implementation Plan ~~for Project 2019-03~~”

- CIP-013-~~2~~3 Technical Rationale

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	
2	08/01/2019	Modified to address directive in FERC Order No. 850.	Revised
2	11/05/2020	Approved by the NERC Board of Trustees.	
2	3/18/2021	FERC Order approving CIP-013-2. Docket No. RD21-2-000.	
2	4/5/2021	Effective Date	10/1/2022
3	TBD	Virtualization Modifications	

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Implementation Plan

Project 2016-02 Modifications to CIP Standards

Applicable Standard(s)

- Reliability Standard CIP-002-7 – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-10 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-8 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-8 – Cyber Security – BES Cyber System Logical Isolation
- Reliability Standard CIP-006-7 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-7 – Cyber Security – System Security Management
- Reliability Standard CIP-008-7 – Cyber Security – Incident Reporting and Response Planning
- Reliability Standard CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-5 – Cyber Security – Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-4 – Cyber Security – Information Protection
- Reliability Standard CIP-013-3 – Cyber Security – Supply Chain Risk Management
- Proposed new or modified terms listed in the “CIP Definitions Project 2016-02 Modifications to CIP Standards Final Draft”.

  These standards and Definitions of Terms used in the versions listed above of the CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

  These standards and new and modified terms used in the standards above will be referenced as the “Revised CIP Standards and Definitions” within the Implementation Plan.

Requested Retirement(s)

- Reliability Standard CIP-002-5.1a – Cyber Security – BES Cyber System Categorization
- Reliability Standard CIP-003-9 – Cyber Security – Security Management Controls
- Reliability Standard CIP-004-7 – Cyber Security – Personnel & Training
- Reliability Standard CIP-005-7 – Cyber Security – Electronic Security Perimeter(s)
- Reliability Standard CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
- Reliability Standard CIP-007-6 – Cyber Security – System Security Management
- Reliability Standard CIP-008-6 – Cyber Security – Incident Reporting and Response Planning

- Reliability Standard CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- Reliability Standard CIP-010-4 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- Reliability Standard CIP-011-3 – Cyber Security – Information Protection
- Reliability Standard CIP-013-2 – Cyber Security – Supply Chain Risk Management

These standards and definitions used in the versions listed above will be referenced as the "Requested CIP Retired Standards" within the Implementation Plan.

Prerequisite Standard(s) or Definitions

These standard(s) or definitions must be approved before the Applicable Standard(s) become effective:

- BES Cyber Asset (BCA)
- BES Cyber System (BCS)
- BES Cyber System Information (BCSI)
- CIP Senior Manager
- Cyber Assets
- Cyber Security Incident
- Cyber System
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Point (EAP)
- External Routable Connectivity (ERC)
- Electronic Security Perimeter (ESP)
- Interactive Remote Access (IRA)
- Intermediate System
- Management Interface
- Physical Access Control Systems (PACS)
- Physical Security Perimeter (PSP)
- Protected Cyber Asset (PCA)
- Removable Media
- Reportable Cyber Security Incident
- Shared Cyber Infrastructure (SCI)
- Transient Cyber Asset (TCA)
- Virtual Cyber Asset (VCA)

Applicable Entities

- Balancing Authority
- Distribution Provider[1]
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

General Considerations

The intent of the Initial Performance of Periodic Requirements section is for Responsible Entities to remain on the same time interval of the prior versions of the standards for their performance of the requirements under the new versions. The intent of the Compliance Dates for Early Adoption of Revised CIP Standards and Definitions section is to permit Responsible Entities the option to comply with the Revised CIP Standards and Definitions prior to the Effective Date. While the Revised CIP Standards and Definitions are designed to be backwards compatible with perimeter-based security, some Responsible Entities may elect to comply early to leverage different security options associated with zero trust architecture.

Effective Date and Phased-in Compliance Dates

The Effective Dates for the Revised CIP Standards and Definitions are provided below. As noted in the General Considerations section above, the standard drafting team determined to clarify initial performance of periodic requirements and permit Responsible Entities to comply with the Revised CIP Standards and Definitions prior to the effective date. These provisions are also provided below.

Revised CIP Standards and Definitions

Where approval by an applicable governmental authority is required, the Revised CIP Standards and Definitions shall become effective on the later of: (1) April 1, 2026; or (2) the first day of the first calendar quarter that is twenty-four (24) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Revised CIP Standards and Definitions shall become effective on the first day of the first calendar quarter that is twenty-four (24) months after the date the Revised CIP Standards and Definitions are adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

---

[1] See Applicability section of Revised CIP Standards and Definitions for additional information on Distribution Providers subject to the standards.

Initial Performance of Periodic Requirements
Responsible Entities shall initially comply with the periodic requirements in the Revised CIP Standards and Definitions within the periodic timeframes of their last performance under the Requested CIP Retired Standards.

Compliance Dates for Early Adoption of Revised CIP Standards and Definitions
A Responsible Entity may elect to comply with the Revised CIP Standards and Definitions following their approval by the applicable governmental authority, but prior to the Effective Date. In such a case, the Responsible Entity shall select one of the following Early Adoption Dates and shall notify the applicable Regional Entities of their selected Early Adoption Date within fifteen (15) calendar days after their selected Early Adoption Date:

Early Adoption Date
Option 1: First day of the first calendar quarter that is six (6) months after the effective date of the applicable governmental authority’s order approving the Revised CIP Standards and Definitions
Option 2: First day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority’s order approving the Revised CIP Standards and Definitions
Option 3: First day of the first calendar quarter that is eighteen (18) months after the effective date of the applicable governmental authority’s order approving the Revised CIP Standards and Definitions

Responsible Entities must comply with applicable Requested CIP Retired Standards until their selected Early Adoption Date. All Responsible Entities, regardless of whether or not they selected an Early Adoption Date, must comply with the Revised CIP Standards and Definitions by the Effective Date.

Planned or Unplanned Changes

Planned Changes

Planned changes refer to any changes of the electric system or BES Cyber System which were planned and implemented by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-7, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

For planned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Unplanned Changes

Unplanned changes refer to any changes of the electric system or BES Cyber System which were not planned by the Responsible Entity and subsequently identified through the annual assessment under CIP-002-7, Requirement R2.

For example, consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-7, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-7, Attachment 1, criteria.

For unplanned changes resulting in a higher categorization, the Responsible Entity shall comply with all applicable requirements in the CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section Initial Performance of Certain Periodic Requirements of the CIP-002-7 Implementation Plan.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirement not applicable to Medium impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 months
Responsible Entity identifies its first high impact or medium impact BES Cyber System (i.e., the Responsible Entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Retirement Date

Requested CIP Retired Standards

The Requested CIP Retired Standards shall be retired immediately prior to the effective date of the Revised CIP Standards and Definitions in the particular jurisdiction in which the Revised CIP Standards and Definitions are becoming effective.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards | Final Draft

The standard drafting team (SDT) is seeking comment on the following new or modified terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised Definition
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the Reliable Operation of the Bulk Electric System (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS) **Update is Acronym only.**	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	
BES Cyber System Information	Information about the BES Cyber System that could be	Information about the BES Cyber System (BCS) that

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
(BCSI)	used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	could be used to gain unauthorized access or pose a security threat to the BCS. BES Cyber System Information (BCSI) does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BCS, such as, but not limited to, device names, individual IP addresses without context, Electronic Security Perimeter names, or policy statements. Examples of BCSI may include, but are not limited to, security procedures or security information about BCS, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BCS.
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Cyber Security Standards.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.	Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: • For a high or medium impact BES Cyber System (BCS), compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring Systems; or (4) Shared Cyber Infrastructure; or • Disrupts or attempts to disrupt the operation of a BCS.
Cyber System ***New Definition***		One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	Cyber System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) (ESP) or BES Cyber Systems (BCS), including those not protected by an ESP used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	An electronic policy enforcement point or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable	The ability to access a BES Cyber System through its Electronic Security Perimeter via a bi-directional routable protocol connection.

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
	protocol connection.	
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated electronic access by a person using a bi-directional routable protocol: • To a Cyber System protected by an Electronic Security Perimeter(s) (ESP); • That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber System; or • To a Management Interface. Interactive Remote Access does not include: • Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or • System-to-system process communication.
Intermediate System	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
Management Interface ***New Definition***		An administrative interface that: • Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; • Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or • Configures an Electronic Access Point.
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers	Cyber Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	One or more Cyber Assets or Virtual Cyber Assets (VCA) that: • Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or • Share CPU resources or memory resources with any part of the BCS, excluding VCA that are being

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
		actively remediated in an environment that isolates routable connectivity from BCS; Excluding Transient Cyber Assets.
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure (SCI), (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, SCI, a network protected by an Electronic Security Perimeter, or a Protected Cyber Asset.
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	A Cyber Security Incident that compromised or disrupted: • A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity; • An Electronic Security Perimeter of a high or medium impact BCS; • An Electronic Access Control or Monitoring Systems of a high or medium impact BCS; or • Shared Cyber Infrastructure supporting a BCS.
Shared Cyber Infrastructure (SCI) ***New Definition***		One or more programmable electronic devices, including the software that shares the devices' resources, that: • Hosts one or more Virtual Cyber Assets (VCA)

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
		included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or • Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization. SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset,	A Cyber Asset or Virtual Cyber Asset (VCA) that is: 1. Capable of transmitting or transferring executable code; 2. Not included in a BES Cyber System (BCS); 3. Not a Protected Cyber Asset (PCA) associated with high or medium impact BCS; and 4. Connected for 30 consecutive calendar days or less: • On a network protected by an Electronic Security Perimeter containing high or medium impact BCS; or

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
	• network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	• Directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a: ▪ BES Cyber Asset; ▪ Shared Cyber Infrastructure; or ▪ PCA associated with high or medium impact BCS. Virtual machines hosted on a physical Transient Cyber Asset (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Virtual Cyber Asset (VCA) ***New Definition***		A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include: • Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems; • Dormant file-based images that contain operating

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition**
		systems or firmware; or • SCI or Cyber Assets that host VCAs. Application containers are considered software of VCAs or Cyber Assets.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards | Final Draft

The standard drafting team (SDT) is seeking comment on the following new or modified terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the ~~reliable operation~~Reliable Operation of the Bulk Electric System~~.~~ (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System (BCS) **Update is Acronym only.**	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	
BES Cyber System Information	Information about the BES Cyber System that could be	Information about the BES Cyber System (BCS) that

Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved
(BCSI)	used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	could be used to gain unauthorized access or pose a security threat to the ~~BES Cyber System.~~BCS. BES Cyber System Information (BCSI) does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to ~~BES Cyber Systems~~BCS, such as, but not limited to, device names, individual IP addresses without context, ~~ESP~~Electronic Security Perimeter names, or policy statements. Examples of ~~BES Cyber System Information~~BCSI may include, but are not limited to, security procedures or security information about ~~BES~~BCS, Shared Cyber ~~Systems~~Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the ~~BES Cyber System~~BCS.
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC ~~CIP~~Critical Infrastructure Protection Cyber Security Standards~~,~~ ~~CIP-002 through CIP-011.~~.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.	Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of

Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved
		Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: ~~-~~For a high or medium impact BES Cyber System~~,~~ (BCS), compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, ~~or~~ (3) an Electronic Access Control or • Monitoring ~~System~~Systems; or (4) Shared Cyber Infrastructure; or • ~~-~~Disrupts or attempts to disrupt the operation of a ~~BES Cyber System~~BCS.
Cyber System ***New Definition***		One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	Cyber ~~Assets~~System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) ~~or BES Cyber Systems. This includes Intermediate Systems.~~(ESP) or BES Cyber Systems (BCS), including those not protected by an ESP used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS.
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic	~~A~~An electronic policy enforcement point or a Cyber Asset interface on an Electronic ~~Security Perimeter~~Access Control or Monitoring Systems that ~~allows~~controls routable communication ~~between~~to

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
	Security Perimeter.	and from one or more BES Cyber Systems or their associated Protected Cyber Assets~~ outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.~~.
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System ~~from a Cyber Asset that is outside of its associated~~through its Electronic Security Perimeter via a bi-directional routable protocol connection.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol~~.~~; or a logical boundary defined by one or more Electronic Access Points.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated electronic access by a person ~~employing a remote access client or other remote access technology~~ using a bi-directional routable protocol~~. Remote access originates from a Cyber Asset that is not an Intermediate~~ : • To a Cyber System ~~and not located within any of the Responsible Entity's~~ protected by an Electronic Security Perimeter(s) ~~or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1)~~ (ESP); • That is converted by the responsible entity to a non-routable protocol that allows access to a Cyber ~~Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by~~

Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved
		~~employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants.~~ System; or • To a Management Interface. Interactive ~~remote access~~ Remote Access does not include ~~system~~: • Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or • System-to-system process ~~communications~~communication.
Intermediate System	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	~~A Cyber Asset~~One or ~~collection of Cyber Assets performing access control~~more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users. ~~The Intermediate System must not be located inside the Electronic Security Perimeter.~~
Management Interface ***New Definition***		An administrative interface that: • Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; • Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system;

Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved
		or - Configures an Electronic Access Point.
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers	Cyber ~~Assets~~Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	One or more Cyber Assets ~~connected using a routable protocol within~~ or ~~on~~Virtual Cyber Assets (VCA) that: - Are protected by an Electronic Security Perimeter ~~that is~~(ESP) but are not part of the highest impact BES Cyber System ~~within~~(BCS) protected by the same ~~Electronic Security Perimeter. The impact rating~~ESP; or - Share CPU resources or memory resources with any part of ~~Protected Cyber Assets is equal to~~ the ~~highest rated BES~~BCS, excluding VCA that are being actively remediated in an environment that isolates routable connectivity from BCS;

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
		Excluding Transient Cyber ~~System in the same ESP.~~Assets.
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets~~,~~ or Shared Cyber Infrastructure (SCI), (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, SCI, a network ~~within~~protected by an ~~ESP~~Electronic Security Perimeter, or a Protected Cyber Asset. ~~Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	A Cyber Security Incident that compromised or disrupted: • ~~-~~A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity; • ~~-~~An Electronic Security Perimeter of a high or medium impact ~~BES Cyber System; or~~BCS; • ~~-~~An Electronic Access Control or Monitoring ~~System~~Systems of a high or medium impact ~~BES~~BCS; or • Shared Cyber ~~System~~Infrastructure supporting a BCS.
Shared Cyber Infrastructure (SCI) ***New Definition***		One or more programmable electronic devices, including the software that shares the devices’

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
		resources, that: • Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or • Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization. SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30	A Cyber Asset or Virtual Cyber Asset (VCA) that is: 1. ~~capable~~Capable of transmitting or transferring executable code~~,~~; 2. ~~not~~Not included in a BES Cyber System~~,~~ (BCS); 3. ~~not~~Not a Protected Cyber Asset (PCA) associated with high or medium impact ~~BES Cyber Systems,~~BCS; and 4. ~~directly connected~~Connected for 30 consecutive calendar days or less:

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
	consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	• On a network protected by an Electronic Security Perimeter containing high or medium impact BCS; or • Directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) ~~for 30 consecutive calendar days or less to a:~~to a: ▪ BES Cyber Asset~~,~~; ~~• network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or~~ ▪ Shared Cyber Infrastructure; or ▪ PCA associated with high or medium impact ~~BES Cyber Systems~~BCS. ~~Examples of~~ Virtual machines hosted on a physical Transient Cyber ~~Assets~~Asset (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Virtual Cyber Asset (VCA) ***New Definition***		A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System;

Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised Definition REDLINE TO Currently Approved**
		Protected Cyber Asset; or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include: • Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems; • Dormant file-based images that contain operating systems or firmware; or • SCI or Cyber Assets that host VCAs. Application containers are considered software of VCAs or Cyber Assets.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Technical Rationale

New and Modified Terms, and Exemption Language Used in NERC Reliability Standards | Project 2016-02 Modifications to CIP Standards

Introduction

The standard drafting team (SDT) has in several terms made changes based on the intent that the glossary is a dictionary and defines what something is, not its security requirements or necessarily the scope of systems those requirements apply to. The rationale for such changes is:

- If scoping of which specific systems is included in the definition, the definition can no longer be used in other standards or other requirements with a differing scope. If what the term defines is needed in a differing requirement of a slightly different scope, either the definition must change affecting all uses of it in all standards, or we proliferate more glossary terms to include differing scopes in the definition. Removing specific scoping in definitions alleviates this concern. Several terms below now use a far more generic 'Cyber System' in the definition with the specific scoping of requirements left to those requirements in the standards.
- If implicit requirements are included in the definition (e.g., such as where in relation to an Electronic Security Perimeter (ESP) an Intermediate System must be implemented), then if an entity implements that one aspect incorrectly, that is non-conformant with a glossary term, the unintended consequence is that it may lead to non-compliance with all requirements that rely on that term. Putting any requirement-type language in requirements rather than definitions alleviates this concern.

Proposed Modified Terms:

BES Cyber Asset (BCA)

A Cyber Asset or Virtual Cyber Asset, that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the Reliable Operation of the Bulk Electric System (BES). Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Rationale

The BCA definition was modified to allow for BCA to be either Cyber Assets (hardware included) or Virtual Cyber Assets (VCA) (software only virtual machines without the underlying hardware). See the VCA and Shared Cyber Infrastructure (SCI) definition below. Note that SCI is not included because if the hardware is supporting VCAs of differing impact levels, it is not a BCA with a single impact category, but it is SCI and subject to the additional "SCI only" requirements. If all the hosted VCAs are treated as "associated PCAs" of the highest impact BCS, then the underlying hardware is no longer SCI and is a BCA of the same impact rating as the highest impact BCS it hosts. The SDT also capitalized the term “Reliable Operation” to tie this to “instability, uncontrolled separation, and cascading” as that is a defined term in the NERC Glossary providing more clarity. Additionally, the glossary term uses the Bulk Power System scope, but the BCA definition uses the specific scope “Reliable Operation of the Bulk Electric System” just as the Reliability Coordinator definition does.

BES Cyber System Information (BCSI)

Information about the BES Cyber System (BCS) that could be used to gain unauthorized access or pose a security threat to the BCS. BCSI does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BCS, such as, but not limited to, device names, individual IP addresses without context, Electronic Security Perimeter names, or policy statements. Examples of BCSI may include, but are not limited to, security procedures or security information about BCS, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BCS.

Rationale

The BCSI definition was modified with conforming changes such that BCSI examples include information about SCI that could be used to gain unauthorized access or pose a security threat to the BCS.

Critical Infrastructure Protection (CIP) Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Cyber Security Standards.

Rationale

The CIP Senior Manager definition was modified by removing explicit reference to the CIP standards as only “CIP-002 through CIP-011” since the body of CIP Cyber Security Standards has grown beyond CIP-011. For example, the CIP Senior Manager also has requirements within CIP-013.

Cyber Assets

Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCA) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.

Rationale

The Cyber Asset definition was modified to explicitly exclude SCI from the definition of Cyber Asset such that SCI is a different hardware class on which the other VCAs of differing impact levels execute. SCI is defined separately such that it can be the object of additional requirements based on its unique risks. The definition is also modified to clarify that ‘Application containers’ (i.e., portable, packaged applications) are considered software of a Cyber Asset (or VCA), though they may have some characteristics of a VCA (a container can be instantiated with its own IP address, etc.). This is because of their packaged quality, typically being updated as a whole and not as individual components, and the limited capabilities that containers have. When viewing applications containers as something to apply CIP Requirements to, the concept breaks down quickly due to the nature of container platforms. Additionally, the capabilities that containers do possess, that would offer services on a network for example, would then exist on the VCA or Cyber Asset that the container is running on and can be controlled as part of the required set of controls for that device. Additionally, executing instances of VCAs are not to be considered simply software or data of the Cyber Asset.

Cyber Security Incident

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System (BCS), compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System, or (4) Shared Cyber Infrastructure; or
- Disrupts or attempts to disrupt the operation of a BCS.

Rationale

The Cyber Security Incident definition was modified to add SCI to the scope of compromised or attempted compromises of, the listed perimeters and systems.

Electronic Access Control or Monitoring Systems (EACMS)

Cyber System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) (ESP) or BES Cyber Systems (BCS), including those not protected by an ESP used by the Responsible Entity to convert routable protocol communications to non-routable communications to a BCS.

Rationale

The EACMS definition was modified to add Cyber Systems so that VCA and SCI are included as two other forms that an EACMS can take. Removed the explicit inclusion of Intermediate Systems as that was moved to the Intermediate Systems definition. Added the inclusion of certain protocol conversion scenarios where the protocol converter is clarified to be an EACMS. This involves a Cyber Asset that does perform electronic access control or monitoring that is also converting from a routable protocol (e.g., IP over Ethernet) to non-routable protocol (e.g., ASCII text over serial) to BCS that are themselves non-routable (serial) only. The SDT intent is this does not include “bump in the wire” type converters (i.e., IP to serial converters) that have no capability to identify users and perform electronic access control or monitoring. It does include those Cyber Assets that users login and select a serial port to then communicate with a BCS and are clearly performing electronic access control or monitoring. In this latter scenario, though the BCS itself is serial non-routable only and therefore has no ESP, the converter is still performing as an EACMS. It may also be performing as an Intermediate System for IRA to the serial only BCS (see changes to the IRA definition).

Electronic Access Point (EAP)

An electronic policy enforcement point or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.

Rationale

As network security moves deeper into the infrastructure, it's no longer necessary to prescribe that network security be performed only at a 'Cyber Asset interface on an ESP' at one point on a network edge. Zero Trust, for example, highly distributes the network security model and is not perimeter-based, and this is incorporated through the addition of "electronic policy enforcement point or". With the added flexibility in CIP-005 to adopt these models in addition to the traditional ESP model, the EAP definition was modified to allow for electronic policy enforcement points and no longer prescribes an architecture. The "one or more" and the "associated PCAs" have been added to clarify that EAPs can control communications to a group and not required per individual system.

External Routable Connectivity (ERC)

The ability to access a BES Cyber System through its Electronic Security Perimeter via a bi-directional routable protocol connection.

Rationale

The ERC definition was modified to allow for zero trust or other network models that are not strictly perimeter or network-border based, thus not having concepts of "inside" or "outside". These concepts are replaced with the language "through its ESP" so that it does not imply a prescriptive network security model. The ERC term is used throughout the CIP Standards within the Applicable Systems column as a scoping mechanism based on the inherent risk associated with ERC as well as to limit the scope of requirements that would require ERC to function. The SDT is maintaining this use of ERC, but also clarifying the relationship between ERC and Interactive Remote Access (IRA) in that a non-routable, serial only BCS (thus with no ESP) may have IRA through a subsequent IP/serial conversion (see changes to IRA definition).

Electronic Security Perimeter (ESP)

The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points.

Rationale

The ESP definition was modified to provide flexibility and the use of various architectures and access control models. The traditional network border ESP remains a valid network security model, however it is no longer the only prescribed model as CIP-005 allows other access control models that are not based on network perimeters such as Zero Trust architectures. The proposed ESP definition retains its current definition but appends "or a logical boundary defined by one or more EAPs" to incorporate models that move away from implicit trust within network perimeters and using network location as a primary factor in access control decisions. In these models, the perimeter shrinks to increasingly more granular levels, potentially down to a process or resource level on a BCS. The proposed definition allows for an ESP to be (a) a border surrounding an isolated network that has no external connectivity and thus no EAPs, (b) static point(s) on a network boundary such as a traditional firewall as an EAP that is enforcing access policies or configurations (e.g., firewall rulesets), (c) many dynamic, short-lived, session-level 'perimeters' established at time of access that are network independent (e.g., users to resources, for example), or (d) hybrid implementations combining elements of more than one model.

The SDT has kept the 'logical border' concept for the "surrounding a network" ESP and used the language "logical boundary" for zero trust models. A 'border' does indeed surround an object, in this case a network, but a 'boundary' may not surround or enclose, it's a line that can be crossed, such as a policy enforcement point controlling access to a resource. The SDT has also updated language in the standards to remove concepts such as 'inside' an ESP and replaced that with more inclusive phrases such as 'protected by' an ESP.

Interactive Remote Access (IRA)

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Entity's Electronic Security Perimeter(s) (ESP);
- That is converted by the Responsible Entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

- Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs;
- System-to-system process communication.

Rationale

The IRA definition was modified in two fundamental ways: (1) to incorporate IRA situations where users outside of any of the Responsible Entity's ESPs have interactive access, using a routable protocol, to a non-routable (e.g., serial) Cyber System through a subsequent IP to serial conversion, and (2) to include Management Interfaces as targets of IRA. Note that the scope of which Cyber Systems and Management Interfaces is contained within the applicable requirements in the standards and are not in the definition. The philosophy is scoping of requirements should be in the requirements to keep the definitions usable in other requirements with a different scope if needed. The references to ownership of the remote client have been removed as they are immaterial to the definition of IRA.

The definition begins with "User-initiated electronic access by a person using a bi-directional routable protocol" to match the human interactive (bi-directional) nature of the access to the requirements that secure such access in CIP-005 R2. For example, a batch process cannot read a multi-factor token and enter its displayed code; that security control is designed for interactive humans initiating a remote access session. Also note the person is using a routable protocol to initiate the access.

The definition outlines three targets of IRA:

1) “To a Cyber System protected by an Entity’s Electronic Security Perimeter(s) (ESP)” covers the typical Cyber System that is connected to a network via a routable protocol and thus is protected by an ESP. In this instance, the remote user is using a routable protocol and is accessing a Cyber System on a routable protocol network, for example in a typical LAN-WAN-LAN, end to end routable protocol communication.
2) “That is converted by the Responsible Entity to a non-routable protocol that allows access to a Cyber System” clarifies IRA scenarios where the user is using a routable protocol to a site where the Responsible Entity then connects that session (e.g., using a gateway or terminal server) to a device’s non-routable serial port to provide interactive remote access to the user. A common example is connecting a serial port on a digital relay in a substation to a terminal server or gateway device which is then connected to a routable network in the substation for the purpose of granting a remote user interactive access to the relay without traveling to the substation. This 2nd target of the definition now clarifies this is IRA even though the device itself may not have an ESP if it is only connected serially.

   Note the clarification and explanation in the EACMS definition above that applies to this scenario. The phrase “converted *by the Responsible Entity*” clarifies certain situations that may involve more than one entity and is best described by an example. Entity 1 has a BCS in a substation or generating resource that Entity 2, a Control Center, needs to access. Entity 2 provides a circuit to Entity 1’s site and provides Entity 1 with a serial cable to connect to their BCS. This phrase clarifies that Entity 1 does not require detailed architectural knowledge of what Entity 2 does upstream with the data once delivered to the serial interface if Entity 1 does not do any conversion to routable protocols. If Entity 2 does convert to routable protocols and does provide IRA, then Entity 2 implements the IRA security controls on their routable protocol portion.
3) “To a Management Interface” adds the Management Interface as a valid target of IRA. Note the scope of Management Interfaces covered by CIP is in the CIP-005 requirements, not in the definition.

The definition then has two exclusions of scenarios that are not IRA:

1) “Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs” carries forward this exclusion from the previous definition and is intended to exclude, for example, the scenario of a Control Center operator within one of the Responsible Entity’s ESPs interacting with field devices within its other ESPs, because for it to meet the IRA definition, IRA must originate from somewhere other than one of the Responsible Entity’s protected ESPs.
2) “System-to-system process communication” carries forward this exclusion from the previous definition to clarify that a process that cannot for instance perform multi-factor authentication using tokens or biometrics is not IRA. It is instead covered by CIP-005 R1.

Note that the definition uses the more generic term Cyber Systems. This is in keeping with using the glossary as a dictionary that merely defines a term, in this case a type of access, but does not create or scope CIP requirements within the definition. The scope is in CIP-005 R2's requirement language. The intent is to create definitions that are scope agnostic so they can be used in multiple standards or requirements with varying scope in each.

Intermediate Systems

One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.

Rationale

The Intermediate System definition was modified by removing embedded requirement language (i.e., where an Intermediate System must reside). That language moved to CIP-005 Requirement R2 within a mandatory requirement. The definition was also updated from a Cyber Asset focus to an EACMS focus to include other forms (i.e., VCA) the Intermediate System may take. This also moves the clarification of "This includes Intermediate Systems" out of the EACMS definition into this one.

Physical Access Control Systems (PACS)

Cyber Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.

Rationale

The PACS definition was modified to use the term Cyber Systems to add VCA and SCI as two other forms that a PACS can take.

Physical Security Perimeter (PSP)

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Rationale

The PSP definition was modified to add SCI as type of Cyber System to be included within a PSP.

Protected Cyber Asset (PCA)

One or more Cyber Assets or Virtual Cyber Assets (VCA) that:

- Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or
- Share CPU resources or memory resources with any part of the BCS, excluding VCAs that are being actively remediated in an environment that isolates routable connectivity from BCS;

Excluding Transient Cyber Assets.

Rationale

The PCA definition was modified to ensure additional implementation scenarios in a virtualized environment that present similar risks to the BCS are accounted for through PCA protections. The PCA definition exists to identify other Cyber Assets or VCAs that must be protected by various CIP requirements due to what they share with a BES Cyber System. This sharing could allow the PCA to be a ‘pivot point’, a location from which to access the BCS. In the past, this sharing was limited to local network connectivity; the PCA being a network peer within the same ESP. With virtualization there is now another aspect of sharing and the PCA definition was modified to include “share CPU resources or memory resources with any part of the BCS” to mitigate the risks of hardware-based vulnerabilities (e.g., Spectre, Meltdown, Rowhammer, Zenbleed, etc.) on SCI. Since virtualization can allow systems of differing trust levels to simultaneously execute on the same hypervisor servers in the hardware underlay and thus share the same CPU resources or memory resources, this addition to the PCA definition requires that those VCAs that do share CPU resources or memory resources with a BCS become associated PCA’s of the BCS. This provides the high water marking of VCAs sharing a single hypervisor’s CPU resources or memory resources. Affinity rules can be used within the virtualization configuration to prevent this situation and keep other VCAs of differing impact levels from becoming associated PCAs. Thus, there is no “mixed mode” allowed on the same CPU resources or memory resources.

Finally, the definition was modified to account for “remediation VLAN” automation of security controls where a VCA may instantiate in a logical network reserved for vulnerability assessment and updates (e.g., OS patches, AV updates, etc.) that limits its connectivity to only remediation resources during the remediation process. Even though it may share CPU resources or memory resources during the remediation, the intent is to exclude the VCA from becoming a PCA while temporarily in this state as its being updated prior to being connected to its production network.

Removable Media

Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure (SCI), (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, SCI, a network protected by an Electronic Security Perimeter, or a Protected Cyber Asset.

Rationale

The Removable Media definition was modified to add SCI as a target of the Removable Media connection and incorporate the new ESP definition (“protected by” rather than “within”).

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BCS;
- An Electronic Access Control or Monitoring System of a high or medium impact BCS; or

- Shared Cyber Infrastructure supporting a BCS.

Rationale

The Reportable Cyber security Incident definition was modified to add compromised or disrupted SCI supporting a BCS as a target.

Transient Cyber Asset (TCA)
A Cyber Asset or Virtual Cyber Asset (VCA) that is:

1. Capable of transmitting or transferring executable code,
2. Not included in a BCS,
3. Not a Protected Cyber Asset (PCA) associated with high or medium impact BCS, and
4. Connected for 30 consecutive calendar days or less:
    - On a network within an Electronic Security Perimeter containing high or medium impact BCS; or
    - Directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a:
        - BES Cyber Asset;
        - Shared Cyber Infrastructure; or
        - PCA associated with high or medium impact BCS.

Virtual machines hosted on a physical Transient Cyber Asset (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Rationale
The TCA definition was modified to add VCA as a form a TCA can take. The SDT is addressing two different transient connection scenarios.

The first scenario is a physical TCA such as a laptop. These TCAs may require older, 32-bit software and OS to connect to and configure older equipment in the field. These are often executed within VM ‘player’ environments on the physical TCA. The SDT asserts these packaged environments in an image file on a physical TCA should not be considered their own distinct virtual TCA and included the statement “Virtual machines hosted on a physical TCA are treated as software on that physical TCA” within the definition. The SDT asserts that a user that is authorized to use the physical TCA should not be required to be separately authorized to execute the software they need to use on the TCA, simply because it’s in an image file and executed in a VM “player” type environment on the TCA. The SDT also asserts that if the user ‘checks out’ a physical laptop TCA to perform a task, it should not be a standard violation if they do not also ‘check out’ any VM images residing on that physical TCA’s disk. The intent is that physical TCA is considered a ‘unit’ to perform a job and not several distinct TCAs on one laptop.

The second scenario is a more recent phenomenon where a service vendor (e.g., a pen-tester or security firm) may send an entity a VCA image (e.g., a vulnerability scanner instance) to temporarily instantiate within their virtualization environment. This VCA may only exist for a few hours and is functionally no different than the vendor bringing a physical laptop and connecting it to a physical network switch to perform the same task as a TCA. This transient VCA is not a part of the entity’s CIP program and is treated as a TCA. This also handles VCAs the entity creates for typical TCA uses but are normally dormant on the same hardware as the BCS (e.g., a VCA with Wireshark for troubleshooting network issues within a virtualized infrastructure).

Additionally, SCI was added as a target to which TCAs can be directly connected.

Proposed New Terms:

Cyber System

One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.

Rationale

The term Cyber System was defined to simplify applicability when referring in the standards or other definitions to all the forms an object may take (Cyber Asset, VCA, or SCI). If other forms are needed in the future, their addition to this one definition can reduce needed edits throughout the standards and definitions where it is used.

Management Interface

An administrative interface that:

- Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure;
- Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or
- Configures an EAP.

Rationale

The term Management Interface was defined so that requirements are established for SCI and EACMS Management Interfaces to target the unique risks for virtualized environments presented by unrestricted access to the Management Interfaces for such environments. With ‘infrastructure as a service’ (IaaS) environments, the management consoles can not only be used to create, but also to destroy or reconfigure virtual servers, networks, switches, firewalls, etc. The term also includes interfaces commonly known as ILO (Integrated Lights Out), that can be used to remotely access the console. It also includes interfaces used to configure an EAP (such as on firewalls or a network switch that is enforcing an ESP between different virtual networks (e.g., VLANs). Note that scoping is included in requirements in the standard, not in the definition.

Shared Cyber Infrastructure (SCI)

One or more programmable electronic devices, including the software that shares the devices’ resources, that:

- Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber System (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control

Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or

- Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also, for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.

SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.

Rationale

The term SCI was defined to separate the underlying hardware from VCAs in the situation where the shared hardware resources support VCAs of varying impact levels. This allows security requirements to be targeted to SCI to address the unique risks of shared hardware. There are many requirements that now include the newly defined term SCI in the "Applicable Systems" column to maintain security level parity with traditional Cyber Assets.

Beyond security level parity with protecting a typical hardware based Cyber Asset, the SCI can have a more significant impact in a virtualized environment since it can host, and therefore impact, multiple virtualized systems of varying impact levels. Because of this capability, some additional controls only apply to SCI, such as the management plane isolation required by the proposed CIP-005. Addressing these unique risks requires separation of the hardware underlay into a separate definition.

The phrase "SCI does not include the supported VCAs or Cyber Assets with which it shares its resources" is included to clarify that, for example, electronic access to a hosted VCA by a user is not electronic access to the SCI on which it executes.

Of note is that shared network devices are not in the scope of this definition. Since network switches and firewalls share their resources by nature, this exclusion avoids pulling all network hardware into scope as SCI. However, network switches and other hardware that does enforce an ESP, such as a network switch configured to host different VLANs to which systems of differing impact levels are connected, comes into scope as an EACMS.

Virtual Cyber Asset (VCA)

A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset, Electronic Access Control or Monitoring System, Physical Access Control System, Protected Cyber Asset, or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include:

- Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems;
- Dormant file-based images that contain operating systems or firmware; and
- SCI or Cyber Assets that host VCAs.

Application containers are considered software of VCAs or Cyber Assets.

Rationale

The term VCA was defined to allow the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined as is the case in the Cyber Asset definition. The NERC Glossary definition of Cyber Asset has a direct tie to its hardware and software (“including the hardware, software, and data in the device”) and assumes the electronic device is self-contained with a one-to-one relationship between a device and its software (including the operating system). This affected the definitions of the “Applicable Systems” terms such as BCS, EACMS, PACS, and PCAs that were all based on the Cyber Asset definition. Because the Reliability Standard is applicable to the aforementioned systems, the security controls for the Cyber Assets also applies to the hardware. The one-to-one relationship between a Cyber Asset and its underlying hardware and software is what virtualization intentionally breaks to increase reliability and resiliency by allowing VCAs to be abstracted from the hardware and therefore able move to any available hardware out of a pool of resources.

The phrase “currently executing on a virtual machine” is used to clarify:

- That a VCA does not include disk image files that are not currently instantiated or executing and are thus providing no functions or services.
- That a “logical instance of an operating system or firmware” only refers to those running on a hypervisor as a virtual machine and does not refer to a locally installed OS or firmware on the hardware.

The definition excludes “logical instances that are being actively remediated…” to allow for automated solutions (such as remediation VLANs) to bring newly instantiated instances into compliance in an isolated environment before they are moved to production networks and begin providing their function or service, at which point they become a VCA.

The phrase “hosted on a BCA, EACMS, PACS, PCA, or SCI” is to clarify that an entity for an “all-in” scenario can still classify the underlying hardware as one or several of these types, yet the VCAs remain their own object subject to requirements and are not simply “software in the device” as in the Cyber Asset definition.

Examples of VCAs may include, but are not limited to, logical instances of the following:

- Operating Systems (Virtual Machines (VM));
- Networking devices such as switches, routers, and load balancers;
- Security appliances such as firewalls and VPN concentrators; and
- Helper appliances with logical connectivity (such as malware detection, plugins, etc.).

The definition also clarifies that ‘Application containers’ (i.e., portable, packaged applications) are considered software of a VCA or Cyber Asset, though they may have some characteristics of a VCA. This is because of their packaged quality, typically being updated as a whole and not as individual components, and the limited capabilities that containers have. When viewing applications containers as something to apply CIP Requirements to, the concept breaks down quickly due to the nature of container platforms. Additionally, the capabilities that containers do possess, that would offer services on a network for example, would then exist on the VCA or Cyber Asset that the container is running on and can be controlled as part of the required set of controls for that device.

Technical Rationale for Exemptions Section:

Rationale for Exemption 4.2.3.1

The term 'Cyber Assets' was replaced with the new proposed term 'Cyber Systems'. Rather than changing this language to a list of all possible forms (Cyber Assets, VCAs, or SCI) as the object of the exemption, the SDT chose to instead use the existing language in the 4.2.3.4 and 4.2.3.5 exemptions such that all five exemptions use a form of 'systems' as their object.

Rationale for Exemption 4.2.3.2 and 4.2.3.3

In 4.2.3.2, the term 'Cyber Assets' was replaced with the new proposed term 'Cyber Systems' which is a new proposed glossary addition. Rather than changing these two exemptions to list all possible forms (Cyber Assets, VCAs, or SCI), the SDT chose to define a new term that incorporates all forms and use it within the multiple exemptions and at other points within the standards.

For 4.2.3.3, the ability to move workloads or VMs seamlessly across different sites for increased resiliency can require different sites to be connected as a flat network without layer 3 ESPs at each discrete site (e.g., a layer 2 adjacency across the sites). A "Super ESP" as it has been historically known is created across the sites and thus an exemption based on having a discrete layer 3 ESP at each site no longer works to exclude, for example, the network transport equipment that may belong to carriers. The SDT included the 4.2.3.3 exemption to further clarify this scenario. Responsible Entities should notice the exemption uses the word "between" – when extending an ESP between geographic locations, CIP-005 requires the confidentiality and integrity protection of the data (typically through encryption) between the relevant PSPs. This exemption then covers the related Cyber Systems "between" those encryption points but does not exclude the endpoints performing the encryption.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — BES Cyber System Categorization

Technical Rationale and Justification for Reliability Standard CIP-002-7

April 2024

RELIABILITY | RESILIENCE | SECURITY

**3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com**

Table of Contents

Technical Rationale for Reliability Standard CIP-002-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-002-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-002-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a SDT. The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Attachment 1 – Impact Rating Criteria

Change Rationale:

In the medium impact rating criterion 2.1 referencing shared BCS for commissioned generation, the SDT has proposed a change to incorporate an earlier approved Request For Interpretation (RFI). The RFI was submitted seeking clarification of Criterion 2.1 of Attachment 1 regarding the use of the phrase "shared BES Cyber Systems." The resulting approved interpretation was introduced as Appendix 1 in CIP-002-5.1a.

The SDT incorporated the interpretation into CIP-002-7 Attachment 1 criterion 2.1 by modifying it to reference "each discrete shared BCS" and removed the RFI appendix from the standard.

Former Background Section from Reliability Standard CIP-002-5.1a

The **Background** section has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

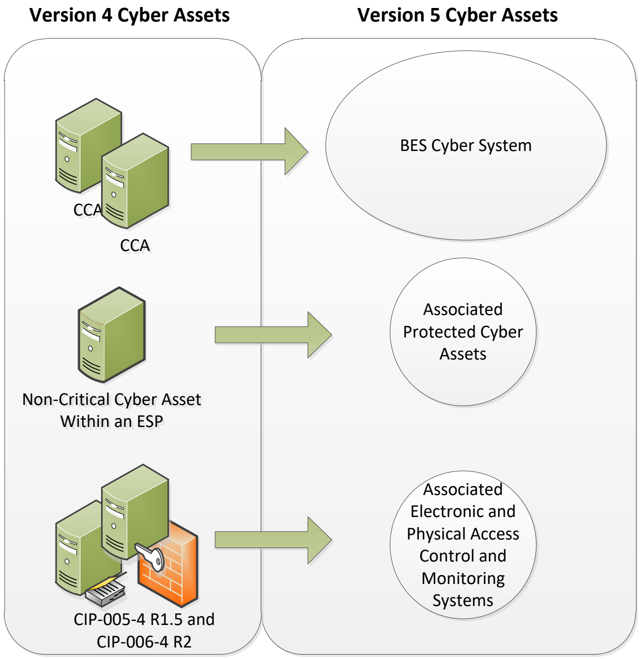
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their Bulk Electric System (BES) Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the BES. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily

to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term “BES Cyber System” is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity’s responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than “Real-time,” BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4, and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS")

Examples include Electronic Access Points, Intermediate Systems, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")

Examples include authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA")

Examples may include, to the extent they are within the ESP file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

Technical Rationale for Reliability Standard CIP-002-5.1a

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from the CIP-002-5.1a standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5.1a and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5.1a. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5.1a

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber Systems that would be subject to CIP-002-5.1a. The concept includes a number of named BES reliability operating services. These named services include:

- Dynamic Response to BES conditions
- Balancing Load and Generation
- Controlling Frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints

- Monitoring & Control
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
    - Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)

        - Special Protection Systems or Remedial Action Schemes
    - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
        - Under and Over Frequency relay protection (includes automatic load shedding)
    - Sensors, relays & breakers (DP)
        - Under and Over Voltage relay protection (includes automatic load shedding)
    - Sensors, relays & breakers (DP)
        - Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions, and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
    - Field data sources (real time tie flows, frequency sources, time error, etc.) (TO, TOP)
    - Software used to perform calculation (BA)
- Demand Response
    - Ability to identify load change need (BA)
    - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
    - Ability to identify load change need (BA)
    - Ability to implement load changes (TOP, DP)
- Non-spinning reserve (contingency reserve)
    - Know generation status, capability, ramp rate, start time (GO, BA)
    - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
    - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
    - Software to calculate unit adjustments (BA)
    - Transmit adjustments to individual units (GOP)
    - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
    - Frequency source, schedule (BA)
    - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions, and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive, or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term “Facilities”, there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” In most cases, the criteria refer to a group of Facilities in a given location that supports

the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5.1a, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.

- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, Bas, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of Bas with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1’s medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is “to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance.” In particular, it requires that “as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency.” The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various Bas in all regions.

In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities’ qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a “long term” reliability planning, i.e. that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as “Reliability Must Run,” and this designation is distinct from those generation Facilities designated as “must run” for market stabilization purposes. Because the use of the term “must run” creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.
- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1.
- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e., fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.
- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

  It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.
- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:
  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

- 230 kV –> 700 MVA
- 345 kV –> 1,300 MVA
- 500 kV –> 2,000 MVA
- 765 kV –> 3,000 MVA

In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

- For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would consider the connections in and out of each station or substation location.
- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.
- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.
- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIRs are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.
- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.
- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise, or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.
- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

  In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.
- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that “control” 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC’s Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

  Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

  BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator’s restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator’s restoration plan. The glossary term Blackstart Capability Plan has been retired.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to “provide the entities identified in

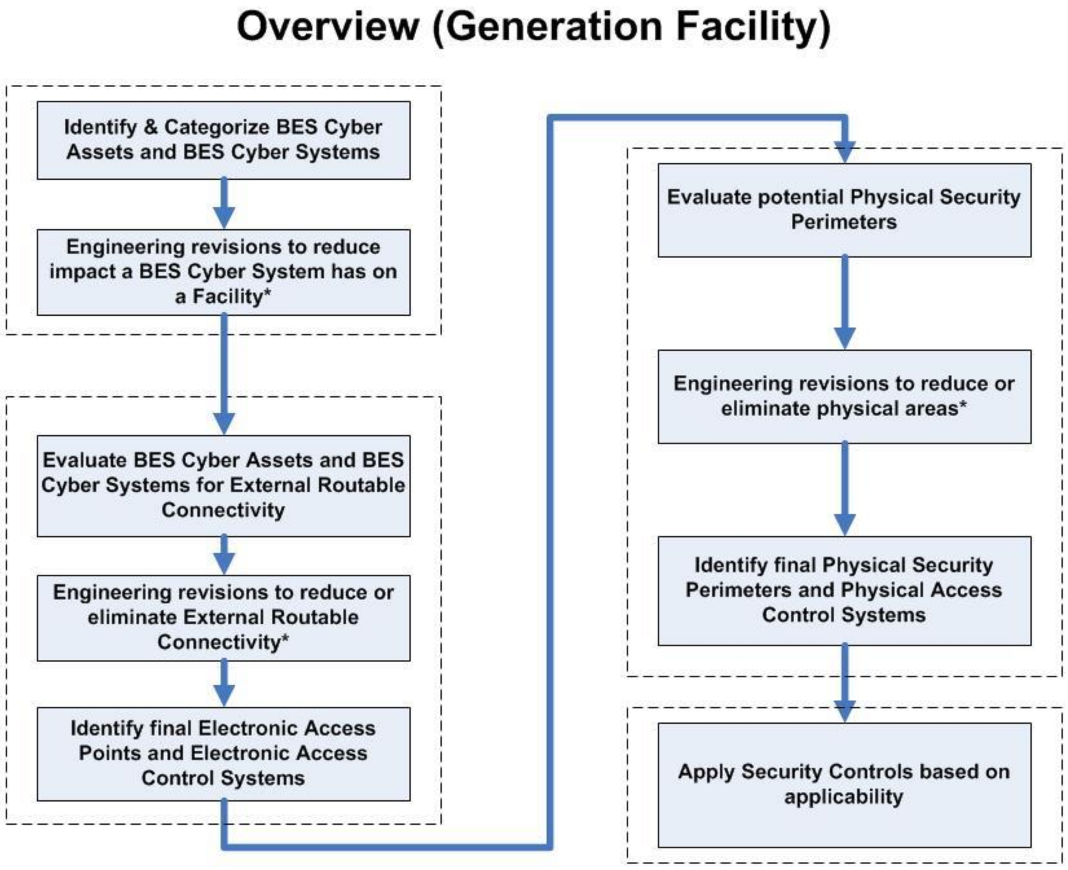
its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the BES. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Appendix 1

Requirement Number and Text of Requirement

CIP-002-5.1, Requirement R1

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3:

i. Control Centers and backup Control Centers;

ii. Transmission stations and substations;

iii. Generation resources;

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;

v. Special Protection Systems that support the reliable operation of the Bulk Electric System; and

vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

Attachment 1, Criterion 2.1

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

Questions

Energy Sector Security Consortium, Inc. (EnergySec) submitted a Request for Interpretation (RFI) seeking clarification of Criterion 2.1 of Attachment 1 in Reliability Standard CIP-002-5.1 regarding the use of the phrase “shared BES Cyber Systems.”

The Interpretation Drafting Team identified the following questions in the RFI:

1. Whether the phrase “shared BES Cyber Systems” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?
2. Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?
3. If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

Responses

Question 1: Whether the phrase “shared BES Cyber Systems,” means that the evaluation for Criterion 2.1 shall be performed individually for each discrete BES Cyber System at a single plant location, or collectively for groups of BES Cyber Systems?

The evaluation as to whether a BES Cyber System is shared should be performed individually for each discrete BES Cyber System. In the standard language of CIP-002-5.1, there is no reference to or obligation to group BES Cyber Systems. Requirement R1, part 1.2 states “Identify *each* of the medium impact BES Cyber Systems according to Attachment 1, Section 2…” Further, the preamble of Section 2 of CIP-002-5.1 Attachment 1 states “*Each BES Cyber System*…associated with any of the following [criteria].” (emphasis added)

Additionally, the Background section of CIP-002-5.1 states that “[i]t is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System.” The Background section also provides:

> The Responsible Entity should take into consideration the operational environment and scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Question 2: Whether the phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple units, or groups of BES Cyber Systems that could collectively impact multiple units?

The phrase “shared BES Cyber Systems” refers to discrete BES Cyber Systems that are shared by multiple generation units.

The use of the term “shared” is also clarified in the NERC Frequently Asked Questions (FAQ) document issued by NERC Compliance to support implementation of the CIP Reliability Standards. FAQ #49 provides:

> Shared BES Cyber Systems are those that are associated with any combination of units in a single Interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criterion 2.1 “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.” For criterion 2.2: “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR. Also refer to the Lesson Learned for CIP-002-5.1 Requirement R1: **Impact Rating of Generation Resource Shared BES Cyber Systems** for further information and examples.

Question 3: If the phrase applies collectively to groups of BES Cyber Systems, what criteria should be used to determine which BES Cyber Systems should be grouped for collective evaluation?

The phrase applies to each discrete BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Security Management Controls

Technical Rationale and Justification for Reliability Standard CIP-003-10

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-003-10

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-10. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-10 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document stated, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-10 to shorten applicability statements within the body of CIP standards with "BCS" as the defined acronym for "BES Cyber System".

Requirement R2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-10 to align security management control requirements with the virtualization changes.

To ensure SCI supporting low impact BCS is afforded equal security controls as the BCS, the SDT added "SCI that supports a low impact BCS". Where shared infrastructure is serving only low impact BCS it would not meet the 2nd component of the first bullet in the SCI definition and therefore would not qualify as SCI; However, in this scenario the shared infrastructure becomes a component of the low impact BCS and would remain subject to the Requirements within R2.

Attachment 1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-10 to shorten applicability statements within the body of CIP standards with "BCS" as the defined acronym for "BES Cyber System".

To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a system(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term system(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Attachment 1 Section 2

Rationale

To ensure virtual infrastructure providing electronic access controls for the low impact BCS is afforded equal physical security controls as the physical Cyber Assets that provide electronic access controls for the low impact BCS, the SDT modified this section to include the Virtual Cyber Asset (VCA) where only Cyber Assets had previously been listed.

Attachment 1 Section 3 Part 3.1

Rationale

Part 3.1(i)

To ensure an asset containing a low impact BCS or an SCI supporting a low impact BCS is afforded equal electronic access controls as the low impact BCS, the SDT added "SCI that supports a low impact BCS and a Cyber System(s) outside the asset containing the low impact BES Cyber System (BCS); or the SCI that supports a low impact BCS"".

To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the SDT adjusted the language to refer to communications that are between a low impact BCS and a Cyber System(s) outside the asset containing low impact BCS, instead of discrete Cyber Assets outside the assets containing low impact BCS. The use of the term Cyber System(s) no longer restricts this section to physical Cyber Assets, thereby permitting VCAs as part of the BCS grouping under the modified definition.

Part 3.1(ii) To ensure only necessary inbound and outbound electronic access is permitted for SCI that supports a low impact BCS just as is required for access control to the low impact BCS, the SDT adjusted the language to include communications that are between SCI that supports any part of a low impact BCS and a system(s) outside the asset(s) containing the SCI that supports any part of a low impact BCS.

Part 3.1 (iii) The SDT replaced the undefined 'intelligent electronic devices' with the defined term 'Protection Systems'.

Attachment 1 Section 3 Part 3.2

Rationale

To ensure SCI supporting low impact BCS are afforded equal electronic access controls for Dial-up Connectivity, the SDT added "or SCI that supports a low impact BCS". To stay in keeping with the systems concept and the exclusion for a discrete list of Cyber Assets, while enabling the use of Virtual Cyber Assets (VCAs), the ‘per Cyber Asset capability’ was changed to ‘per system capability’.

Attachment 1 Section 5 Part 5.2

Rationale

The final bullet of Attachment 1 Section 5 Part 5.2.1 was preceded with the language “Review of” to make the requirement for other methods parallel to the five options listed above it.

Attachment 1 Section 5 Part 5.3

Rationale

To enable for virtualization technologies and capabilities the SDT added, “or VCA” in Attachment 1 Section 5 Parts 5.3.1.

To ensure SCI supporting a low impact BCS are afforded equal protections from malicious code when using Removable Media, the SDT added “SCI that supports a low impact BCS” to the low impact BCS in Attachment 1 Section 5 Parts 5.3.1 & 5.3.2.

Attachment 2

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-003-10 to shorten applicability statements within the body of CIP standards with “BCS” as the defined acronym for “BES Cyber System”. Additional changes were to align the Attachment 2 Measures with the modifications to the Attachment 1 requirement language.

Technical Rationale for Reliability Standard CIP-003-9

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-003-9 standard to preserve any historical references. No modifications have been made.

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-003-9. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-003-9 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2020-03 – Supply Chain Low Impact Revisions Standards Drafting Team (SDT) intent in drafting changes to the requirement.

Background

In its final report[1] accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact Bulk Electric System (BES) Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through Member Representatives Committee (MRC) Policy Input.

After considering policy input, the NERC Board adopted a resolution[2] to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

Foreword Regarding Section 3 and Section 6

When developing the standards language for this SAR, the SDT considered many variables and inputs to draft clear, concise, and meaningful requirements. The SDT considered the scope and variety of entity sizes, functions, organizations, systems and configurations, entity business processes, remote access, local electronic access, remote access architectures and technologies, and data path and communications protocols. The SDT discussed systems used for electronic access, remote vs local electronic access, vendor access accounts and privileges, and optimal time frames for establishing, identifying, determining, and disabling or terminating vendor electronic access.

---

[1] Supply Chain Risk Assessment Report (nerc.com)

[2] FINAL_Minutes_BOT_Open_Meeting_February_2020.pdf (nerc.com)

The SDT reviewed industry comments and draft language suggestions, existing standards, and discussed and deliberated the options and their potential impacts and interpretative values to industry. The SDT recognized that some entities may use the same process, system and/or technology (for vendor electronic access) that is used by entity personnel, or cases where entities use separate processes, systems, or technologies to manage vendor electronic access. The SDT also discussed systems and Cyber Assets owned by vendors but authorized for use on entity networks, vs systems and Cyber Assets owned by entities but used by vendors for electronic remote access. Because of the variety, the SDT focused on allowing entities to identify their particular risks related to remote vendor electronic access and define processes and plans to define and implement security controls to address those risks.

In reviewing the industry comments, the SDT identified, discussed and considered additional terms for clarification, and came to the following conclusions:

1. Electronic remote access: considered remote access as definition and/or remote access vs electronic remote access - as well as onsite vs off-premises remote access. The use of electronic remote access clarifies the remote access using a method (non-physical) which matches existing electronic remote access in other CIP standards.
2. Interactive Remote Access: avoided the existing NERC Glossary of Terms definition in order to prevent applying high and medium impact requirements upon low impact assets and systems.
3. Active: avoided using this term due to potential unintended consequences. The use of “active” may add further requirements upon entities to define, track and document when “active” occurs vs when it does not.
4. Read-only: avoided using this term due to potential unintended consequences. The use of “read-only” may add further requirements upon entities to define and document systems and processes which are read-only from read-write, and where and when read-only access occurs.
5. Vendor: CIP-013 Supplemental Material[3] addresses the term vendor in context with applicable high and medium BES Cyber Systems. The SDT avoided defining the term vendor specifically within the low impact standards to avoid conflicts for entities with high, medium, and low impact systems.

The language developed gives entities the flexibility to define processes to identify and manage vendor electronic remote access for their specific policies, processes, systems, configurations, organizations, operations, and BES Facilities. The language allows entities to define how and where vendor electronic remote access occurs and the ideal methods and timeframes to authorize, establish, and disable vendor electronic remote access.

The SDT agreed to retain Section 3 of CIP-003-9 Requirement R2, Attachment 1 and established Section 6 to specifically address low impact vendor electronic remote access, as well as malicious inbound and outbound data communications which may be sourced from or transmitted to vendors. Based on the SAR, the SDT did not include dial-up from Section 3.2.

The language requires an entity to develop and implement a process or processes for identifying vendor electronic remote access, having a method or methods for disabling vendor electronic remote access, as well as methods to detect known or suspicious vendor inbound and outbound malicious communications.

Entities may choose to define systems, applications and/or configurations used by vendors, accounts and privileges, network data communication paths or physical processes for establishing and disabling vendor electronic remote communications. Section 6 provides the flexibility to meet many types of vendor electronic remote access configurations while managing vendor electronic remote access risks.

---

[3] CIP-013 Technical Rationale

Rationale Section 6 of Attachment 1 (Requirement R2)

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In February 2020, the NERC Board approved the initiation of a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine vendor electronic remote access is initiated; and (3) disable vendor electronic remote access when necessary.

As published in the December 2019 NERC Report: Supply Chain Risk Assessment – Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request, of the 87% of section 1600 data request respondents with low impact BES Cyber Systems approximately 66% have external connectivity which often results in the allowance of vendor electronic remote access. As our grid has grown more complex, the use of external parties to support and maintain low impact BES Cyber Systems, equipment and facilities is expected. However, the prevalence of external connectivity across low-impact BES systems could pose a significant impact to the reliability of the grid through the potential of a common supply chain vulnerability. To address this vulnerability, the originating FERC Order[4], and the resulting NERC Board resolution[5], the proposed Attachment 1 Section 6, as it relates to the existing Requirement R2, mandates that applicable entities develop, document, and implement a process to mitigate the risks associated with malicious communications and vendor electronic remote access.

Attachment 1 Section 6 Part 6.1 – Determining vendor electronic remote access

The objective of Attachment 1 Section 6.1 is for entities to determine vendor electronic remote access to their low impact BES Asset(s) and/or BES Cyber Systems. Such visibility increases an entity’s ability to detect, respond, and resolve issues that may originate with, or be tied to, a particular vendor’s electronic remote access. The obligation in Section 6.1 requires that entities have one or more methods for determining vendor electronic remote access.

Attachment 1 Section 6 Part 6.2 – Disabling vendor electronic remote access

The objective of Attachment 1 Section 6.2 is for entities to have the ability to disable vendor electronic remote access for any basis the entity may choose and to prevent security events and propagation of potential malicious communications which may degrade or have adverse effects upon the entity’s assets containing low impact BES Cyber Systems. The obligation in Section 6.2 requires that entities have a method to disable vendor electronic remote access, which in turn supports the security objective to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Attachment 1 Section 6 Part 6.3 – Detecting known or suspected malicious communications for both inbound and outbound communications

The objective of Attachment 1 Section 6.3 is for entities to have the ability to detect known or suspected malicious communications from vendors, such that the entity may respond to and remediate any resulting adverse impacts.

This sub section is scoped to focus only on vendors’ communications per the NERC Board resolution and the supply chain report. The obligation in Section 6.3 requires that entities must establish a method(s) to detect known or suspected malicious communications from vendors and the systems used by vendors to communicate with assets containing low impact BES Cyber Systems.

---

[4] Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016).

[5] Resolution-Supply Chain Recommendations - Board Approved - February 6, 2020 (LINK)

Current obligations in CIP-003-8 Requirement R2 that govern direct electronic communications with low impact BES Cyber Systems are not as robust as those in CIP-005-6 that govern high impact medium impact BES Cyber Systems. Security controls such as use of Intermediate Systems and multi-factor authentication provide additional security protection from malicious communication and overall access controls for high and medium impact BES Cyber Systems. In addition to Intermediate Systems and multi-factor authentication, high and medium impact BES Cyber Systems at Control Centers have requirements to detect malicious communications at the Electronic Access Points of those systems. These security measures are not required at low impact BES Cyber Systems.

In keeping with the NERC stated risk-based model, there may be a scenario where a vendor directly communicates with a low impact BES Cyber System. In the event that this connection may be compromised, the inclusion of security requirements to detect malicious communications under CIP-003-9 Attachment 1 Section 6 would provide entities visibility and opportunity in detecting and mitigating risks posed by vendor communications.

Former Background from Reliability Standard CIP-003-8

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background
Standard CIP-003 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.

The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements.

The terms program and plan are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term program may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Reliability Standards could also be referred to as a program. However, the terms program and plan do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high, medium, and low impact BES Cyber Systems. For example, a single cyber security awareness program could meet the requirements across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within Regional Reliability Standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Technical Rationale for Reliability Standard CIP-003-8

This section contains a “cut and paste” of the former Guidelines and Technical Basis (GTB) as-is of from CIP-003-8 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

In developing policies in compliance with Requirement R1, the number of policies and their content should be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-8, Requirement R1.

If a Responsible Entity has any high or medium impact BES Cyber Systems, the one or more cyber security policies must cover the nine subject matter areas required by CIP-003-8, Requirement R1, Part 1.1. If a Responsible Entity has identified from CIP-002 any assets containing low impact BES Cyber Systems, the one or more cyber security policies must cover the six subject matter areas required by Requirement R1, Part 1.2.

Responsible Entities that have multiple-impact rated BES Cyber Systems are not required to create separate cyber security policies for high, medium, or low impact BES Cyber Systems. The Responsible Entities have the flexibility to develop policies that cover all three impact ratings.

Implementation of the cyber security policy is not specifically included in CIP-003-8, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-003 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements in NERC cyber security Reliability Standards, but to develop a holistic cyber security policy appropriate for its organization. Elements of a policy that extend beyond the scope of NERC's cyber security Reliability Standards will not be considered candidates for potential violations although they will help demonstrate the organization's internal culture of compliance and posture towards cyber security.

For Part 1.1, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for medium and high impact BES Cyber Systems, if any:

1.1.1 Personnel and training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components
- Availability of system backups

1.1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

For Part 1.2, the Responsible Entity may consider the following for each of the required topics in its one or more cyber security policies for assets containing low impact BES Cyber Systems, if any:

1.2.1 Cyber security awareness

- Method(s) for delivery of security awareness
- Identification of groups to receive cyber security awareness

1.2.2 Physical security controls

- Acceptable approach(es) for selection of physical security control(s)

1.2.3 Electronic access controls

- Acceptable approach(es) for selection of electronic access control(s)

1.2.4 Cyber Security Incident response

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.2.5 Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

- Acceptable use of Transient Cyber Asset(s) and Removable Media

- Method(s) to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media
- Method(s) to request Transient Cyber Asset and Removable Media

1.2.6 Declaring and responding to CIP Exceptional Circumstances

- Process(es) to declare a CIP Exceptional Circumstance
- Process(es) to respond to a declared CIP Exceptional Circumstance

Requirements relating to exceptions to a Responsible Entity's security policies were removed because it is a general management issue that is not within the scope of a reliability requirement. It is an internal policy requirement and not a reliability requirement. However, Responsible Entities are encouraged to continue this practice as a component of their cyber security policies.

In this and all subsequent required approvals in the NERC CIP Reliability Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

The intent of Requirement R2 is for each Responsible Entity to create, document, and implement one or more cyber security plan(s) that address the security objective for the protection of low impact BES Cyber Systems. The required protections are designed to be part of a program that covers the low impact BES Cyber Systems collectively at an asset level (based on the list of assets containing low impact BES Cyber Systems identified in CIP-002), but not at an individual device or system level.

Requirement R2, Attachment 1

As noted, Attachment 1 contains the sections that must be included in the cyber security plan(s). The intent is to allow entities that have a combination of high, medium, and low impact BES Cyber Systems the flexibility to choose, if desired, to cover their low impact BES Cyber Systems (or any subset) under their programs used for the high or medium impact BES Cyber Systems rather than maintain two separate programs. The purpose of the cyber security plan(s) in Requirement R2 is for Responsible Entities to use the cyber security plan(s) as a means of documenting their approaches to meeting the subject matter areas. The cyber security plan(s) can be used to reference other policies and procedures that demonstrate "how" the Responsible Entity is meeting each of the subject matter areas, or Responsible Entities can develop comprehensive cyber security plan(s) that contain all of the detailed implementation content solely within the cyber security plan itself. To meet the obligation for the cyber security plan, the expectation is that the cyber security plan contains or references sufficient details to address the implementation of each of the required subject matters areas.

Guidance for each of the subject matter areas of Attachment 1 is provided below.

Requirement R2, Attachment 1, Section 1 – Cyber Security Awareness

The intent of the cyber security awareness program is for entities to reinforce good cyber security practices with their personnel at least once every 15 calendar months. The entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics. As evidence of compliance, the Responsible Entity should be able to produce the awareness material that was delivered according to the delivery method(s) (e.g., posters, emails, or topics at staff meetings, etc.). The standard drafting team does not intend for Responsible Entities to be required to maintain lists of recipients and track the reception of the awareness material by personnel.

Although the focus of the awareness is cyber security, it does not mean that only technology-related topics can be included in the program. Appropriate physical security topics (e.g., tailgating awareness and protection of badges for physical security, or "If you see something, say something" campaigns, etc.) are valid for cyber security awareness. The intent is to cover topics concerning any aspect of the protection of BES Cyber Systems.

Requirement R2, Attachment 1, Section 2 – Physical Security Controls

The Responsible Entity must document and implement methods to control physical access to (1) the asset or the locations of low impact BES Cyber Systems within the asset, and (2) Cyber Assets that implement the electronic access control(s) specified by the Responsible Entity in Attachment 1, Section 3.1, if any. If these Cyber Assets implementing the electronic access controls are located within the same asset as the low impact BES Cyber Asset(s) and inherit the same physical access controls and the same need as outlined in Section 2, this may be noted by the Responsible Entity in either its policies or cyber security plan(s) to avoid duplicate documentation of the same controls.

The Responsible Entity has the flexibility to select the methods used to meet the objective of controlling physical access to (1) the asset(s) containing low impact BES Cyber System(s) or the low impact BES Cyber Systems themselves and (2) the electronic access control Cyber Assets specified by the Responsible Entity, if any. The Responsible Entity may use one or a combination of physical access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or more granular areas of physical access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses.

The security objective is to control the physical access based on need as determined by the Responsible Entity. The need for physical access can be documented at the policy level. The standard drafting team did not intend to obligate an entity to specify a need for each physical access or authorization of an individual for physical access.

Monitoring as a physical security control can be used as a complement or an alternative to physical access control. Examples of monitoring controls include, but are not limited to: (1) alarm systems to detect motion or entry into a controlled area, or (2) human observation of a controlled area. Monitoring does not necessarily require logging and maintaining logs but could include monitoring that physical access has occurred or been attempted (e.g., door alarm, or human observation, etc.). The standard drafting team's intent is that the monitoring does not need to be per low impact BES Cyber System but should be at the appropriate level to meet the security objective of controlling physical access.

User authorization programs and lists of authorized users for physical access are not required although they are an option to meet the security objective.

Requirement R2, Attachment 1, Section 3 – Electronic Access Controls

Section 3 requires the establishment of electronic access controls for assets containing low impact BES Cyber Systems when there is routable protocol communication or Dial-up Connectivity between Cyber Asset(s) outside of the asset containing the low impact BES Cyber System(s) and the low impact BES Cyber System(s) within such asset. The establishment of electronic access controls is intended to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity.

When implementing Attachment 1, Section 3.1, Responsible Entities should note that electronic access controls to permit only necessary inbound and outbound electronic access are required for communications when those communications meet all three of the criteria identified in Attachment 1, Section 3.1. The Responsible Entity should evaluate the communications and when all three criteria are met, the Responsible Entity must document and implement electronic access control(s).

When identifying electronic access controls, Responsible Entities are provided flexibility in the selection of the electronic access controls that meet their operational needs while meeting the security objective of allowing only necessary inbound and outbound electronic access to low impact BES Cyber Systems that use routable protocols between a low impact BES Cyber System(s) and Cyber Asset(s) outside the asset.

In essence, the intent is for Responsible Entities to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset or Dial-up Connectivity to the low impact BES Cyber System(s). Where such communication is present, Responsible Entities should document and implement electronic access control(s). Where routable protocol communication for time-sensitive protection or control functions between intelligent electronic devices that meets the exclusion language is present, Responsible Entities should document that communication, but are not required to establish any specific electronic access controls.

The inputs to this requirement are the assets identified in CIP-002 as containing low impact BES Cyber System(s); therefore, the determination of routable protocol communications or Dial-up Connectivity is an attribute of the asset. However, it is not intended for communication that provides no access to or from the low impact BES Cyber System(s), but happens to be located at the asset with the low impact BES Cyber System(s), to be evaluated for electronic access controls.

Electronic Access Control Exclusion

In order to avoid future technology issues, the obligations for electronic access controls exclude communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions, such as IEC TR-61850-90-5 R-GOOSE messaging. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by the required electronic access controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles. A Responsible Entity using this technology is not expected to implement the electronic access controls noted herein. This exception was included so as not to inhibit the functionality of the time-sensitive characteristics related to this technology and not to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Considerations for Determining Routable Protocol Communications

To determine whether electronic access controls need to be implemented, the Responsible Entity has to determine whether there is communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset.

When determining whether a routable protocol is entering or leaving the asset containing the low impact BES Cyber System(s), Responsible Entities have flexibility in identifying an approach. One approach is for Responsible Entities to identify an “electronic boundary” associated with the asset containing low impact BES Cyber System(s). This is not an Electronic Security Perimeter *per se*, but a demarcation that demonstrates the routable protocol communication entering or leaving the asset between a low impact BES Cyber System and Cyber Asset(s) outside the asset to then have electronic access controls implemented. This electronic boundary may vary by asset type (Control Center, substation, generation resource) and the specific configuration of the asset. If this approach is used, the intent is for the Responsible Entity to define the electronic boundary such that the low impact BES Cyber System(s) located at the asset are contained within the “electronic boundary.” This is strictly for determining which routable protocol communications and networks are internal or inside or local to the asset and which are external to or outside the asset.

Alternatively, the Responsible Entity may find the concepts of what is inside and outside to be intuitively obvious for a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) communicating to a low impact BES Cyber System(s) inside the asset. This may be the case when a low impact BES Cyber System(s) is communicating with a Cyber Asset many miles away and a clear and unambiguous demarcation exists. In this case, a Responsible Entity may decide not to identify an “electronic boundary,” but rather to simply leverage the unambiguous asset demarcation to ensure that the electronic access controls are placed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset.

Determining Electronic Access Controls

Once a Responsible Entity has determined that there is routable communication between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) that uses a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s), the intent is for the Responsible Entity to document and implement its chosen electronic access control(s). The control(s) are intended to allow only “necessary” inbound and outbound electronic access as determined by the Responsible Entity. However the Responsible Entity chooses to document the inbound and outbound access permissions and the need, the intent is that the Responsible Entity is able to explain the reasons for the electronic access permitted. The reasoning for “necessary” inbound and outbound electronic access controls may be documented within the Responsible Entity’s cyber security plan(s), within a comment on an access control list, a database, spreadsheet or other policies or procedures associated with the electronic access controls.

Concept Diagrams

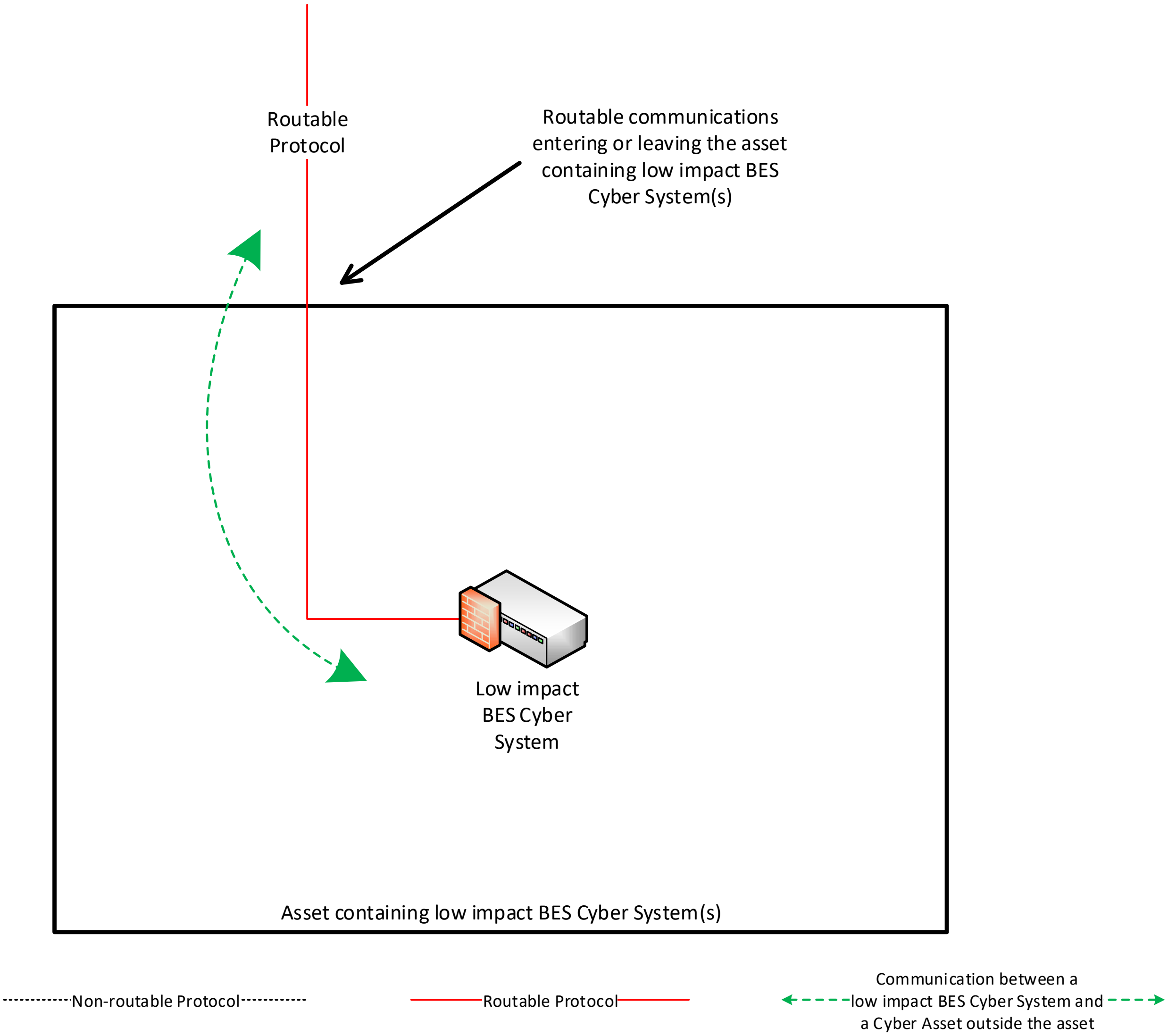
The diagrams on the following pages are provided as examples to illustrate various electronic access controls at a conceptual level. Regardless of the concepts or configurations chosen by the Responsible Entity, the intent is to achieve the security objective of permitting only necessary inbound and outbound electronic access for communication between low impact BES Cyber Systems and Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s) using a routable protocol when entering or leaving the asset.

NOTE:

- This is not an exhaustive list of applicable concepts.
- The same legend is used in each diagram; however, the diagram may not contain all of the articles represented in the legend.

Reference Model 1 – Host-based Inbound & Outbound Access Permissions

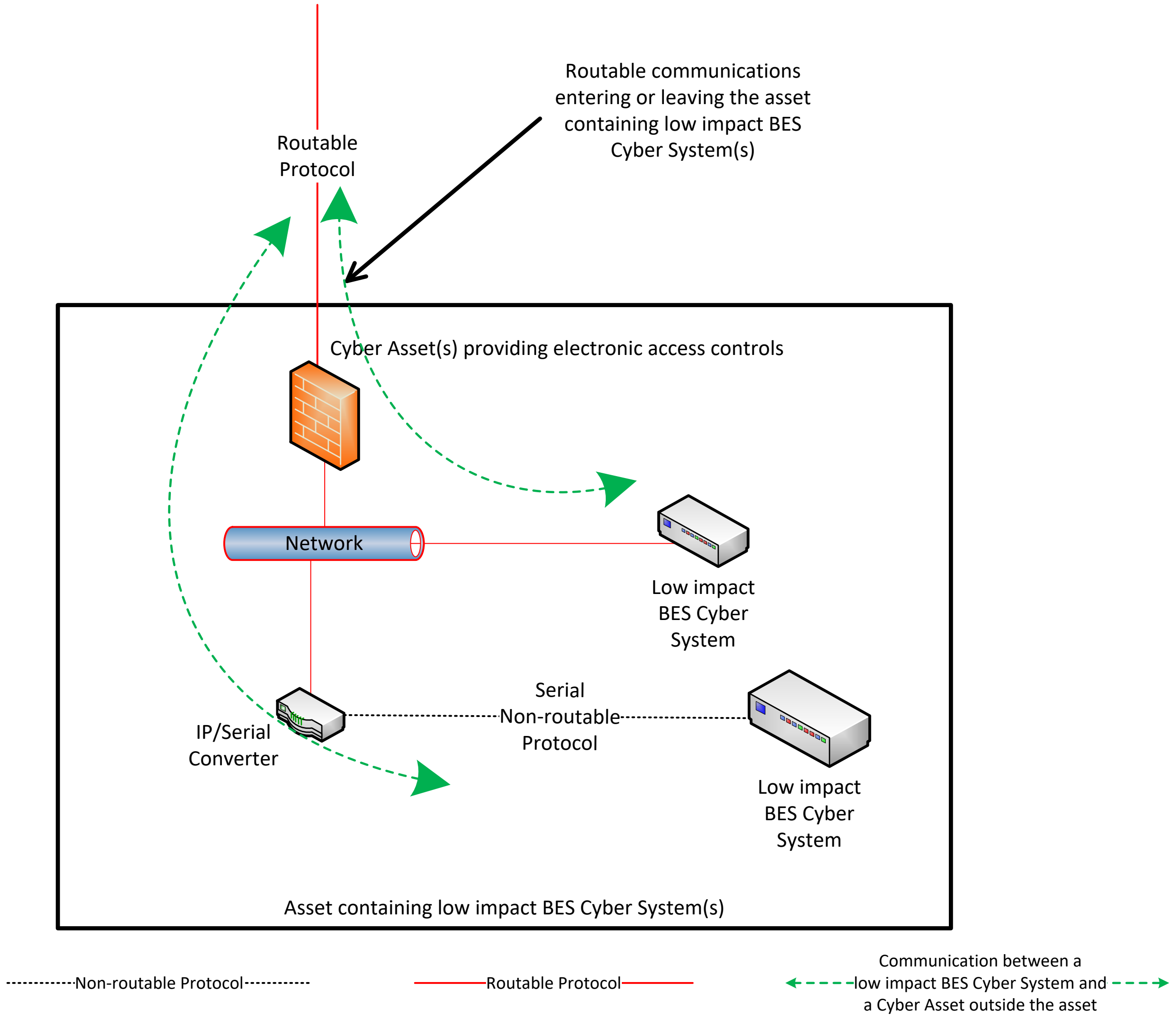
The Responsible Entity may choose to utilize a host-based firewall technology on the low impact BES Cyber System(s) itself that manages the inbound and outbound electronic access permissions so that only necessary inbound and outbound electronic access is allowed between the low impact BES Cyber System(s) and the Cyber Asset(s) outside the asset containing the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 1

Reference Model 2 – Network-based Inbound & Outbound Access Permissions

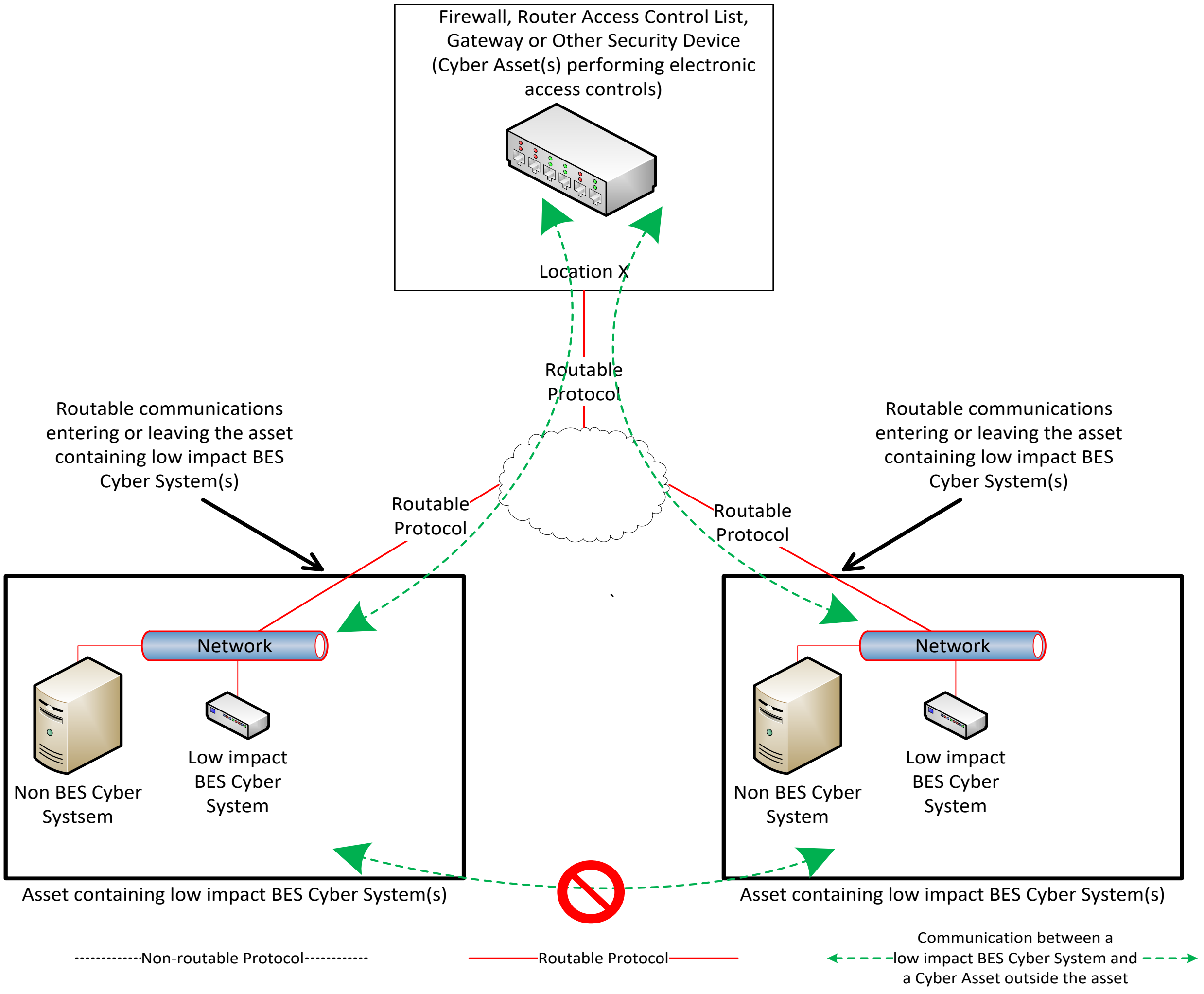
The Responsible Entity may choose to use a security device that permits only necessary inbound and outbound electronic access to the low impact BES Cyber System(s) within the asset containing the low impact BES Cyber System(s). In this example, two low impact BES Cyber Systems are accessed using the routable protocol that is entering or leaving the asset containing the low impact BES Cyber System(s). The IP/Serial converter is continuing the same communications session from the Cyber Asset(s) that are outside the asset to the low impact BES Cyber System(s). The security device provides the electronic access controls to permit only necessary inbound and outbound routable protocol access to the low impact BES Cyber System(s). When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 2

Reference Model 3 – Centralized Network-based Inbound & Outbound Access Permissions

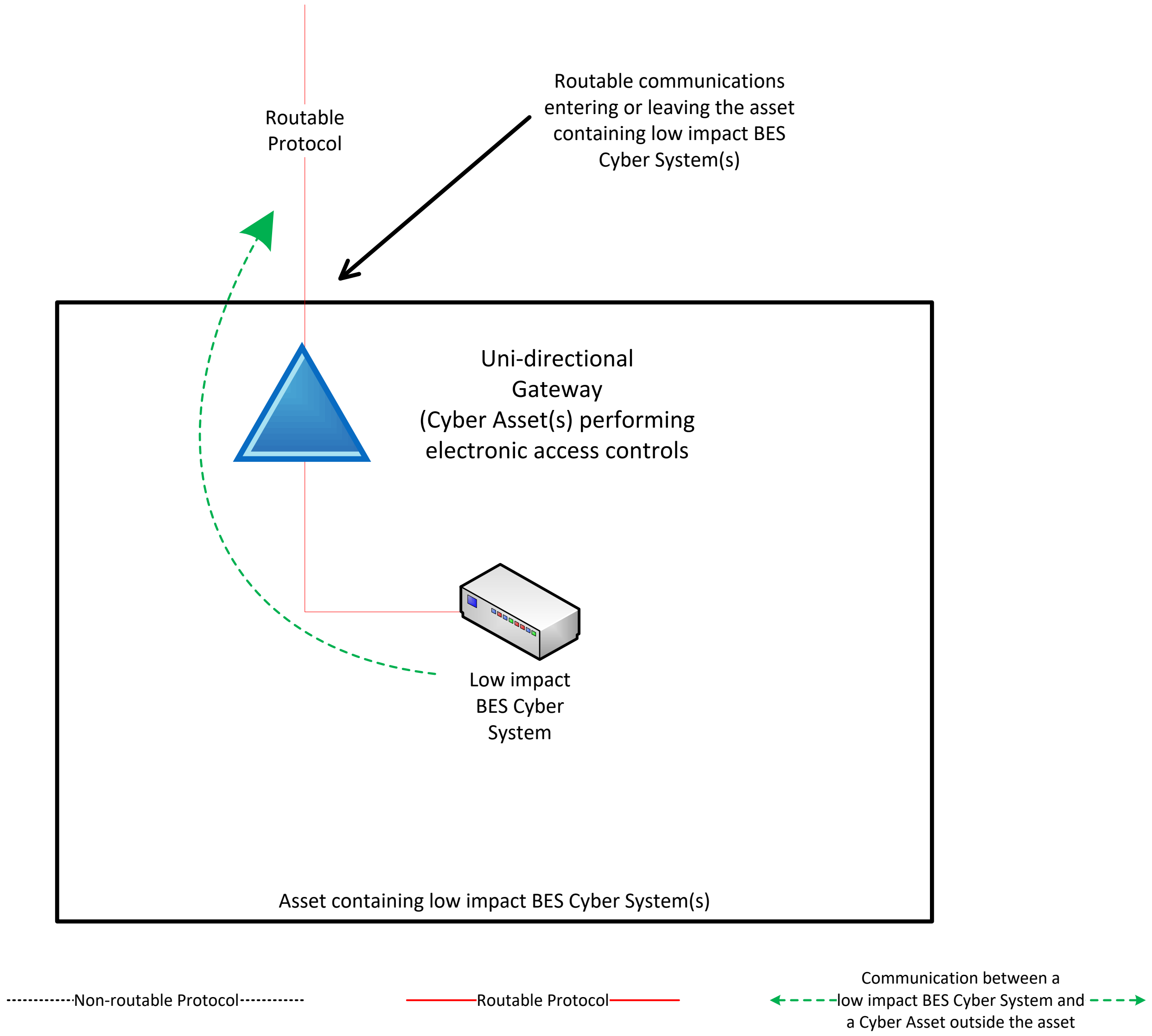
The Responsible Entity may choose to utilize a security device at a centralized location that may or may not be at another asset containing low impact BES Cyber System(s). The electronic access control(s) do not necessarily have to reside inside the asset containing the low impact BES Cyber System(s). A security device is in place at “Location X” to act as the electronic access control and permit only necessary inbound and outbound routable protocol access between the low impact BES Cyber System(s) and the Cyber Asset(s) outside each asset containing low impact BES Cyber System(s). Care should be taken that electronic access to or between each asset is through the Cyber Asset(s) determined by the Responsible Entity to be performing electronic access controls at the centralized location. When permitting the inbound and outbound electronic access permissions using access control lists, the Responsible Entity could restrict communication(s) using source and destination addresses or ranges of addresses. Responsible Entities could also restrict communication(s) using ports or services based on the capability of the electronic access control, the low impact BES Cyber System(s), or the application(s).



Reference Model 3

Reference Model 4 – Uni-directional Gateway

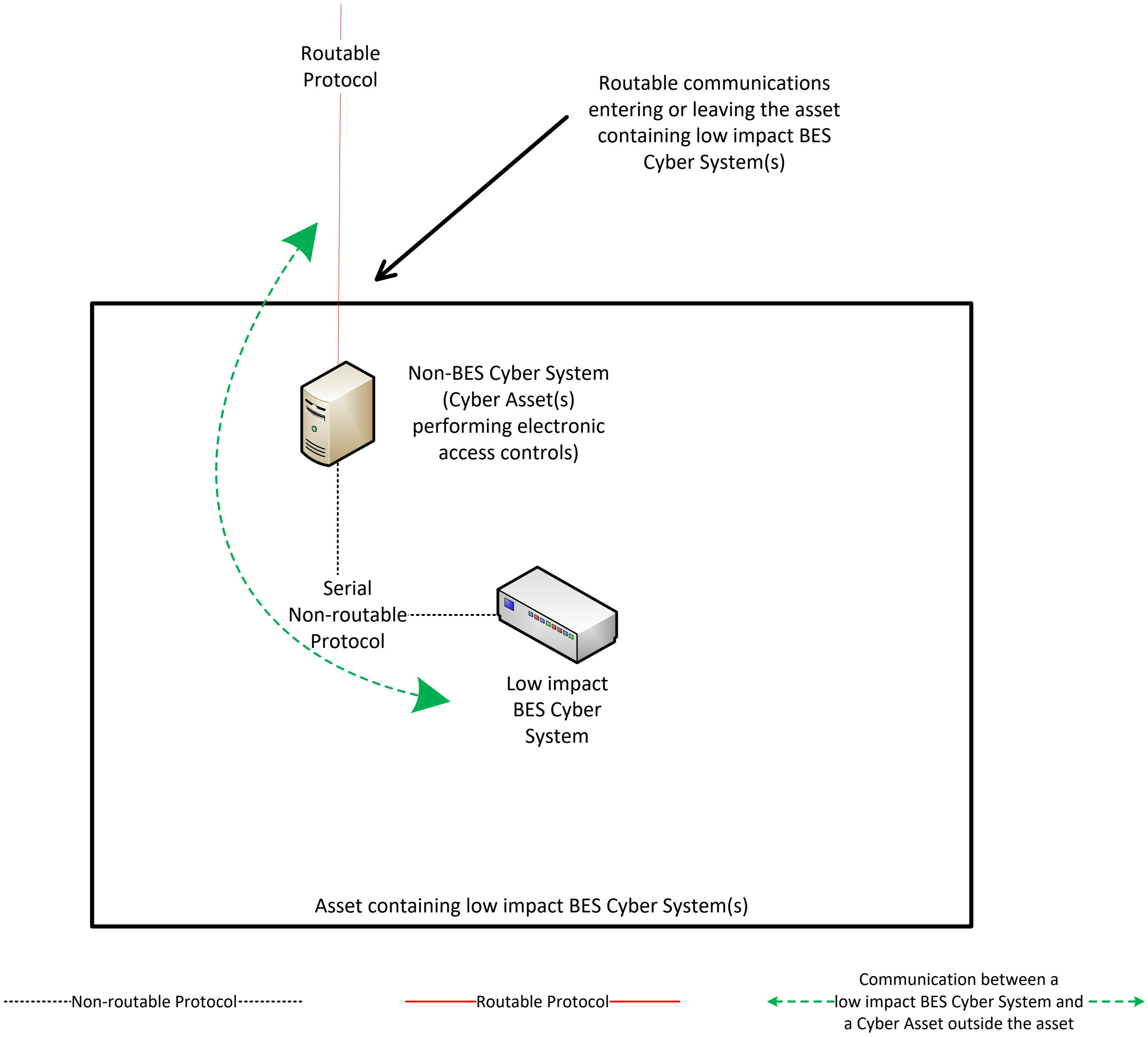
The Responsible Entity may choose to utilize a uni-directional gateway as the electronic access control. The low impact BES Cyber System(s) is not accessible (data cannot flow into the low impact BES Cyber System) using the routable protocol entering the asset due to the implementation of a “one-way” (uni-directional) path for data to flow. The uni-directional gateway is configured to permit only the necessary outbound communications using the routable protocol communication leaving the asset.



Reference Model 4

Reference Model 5 – User Authentication

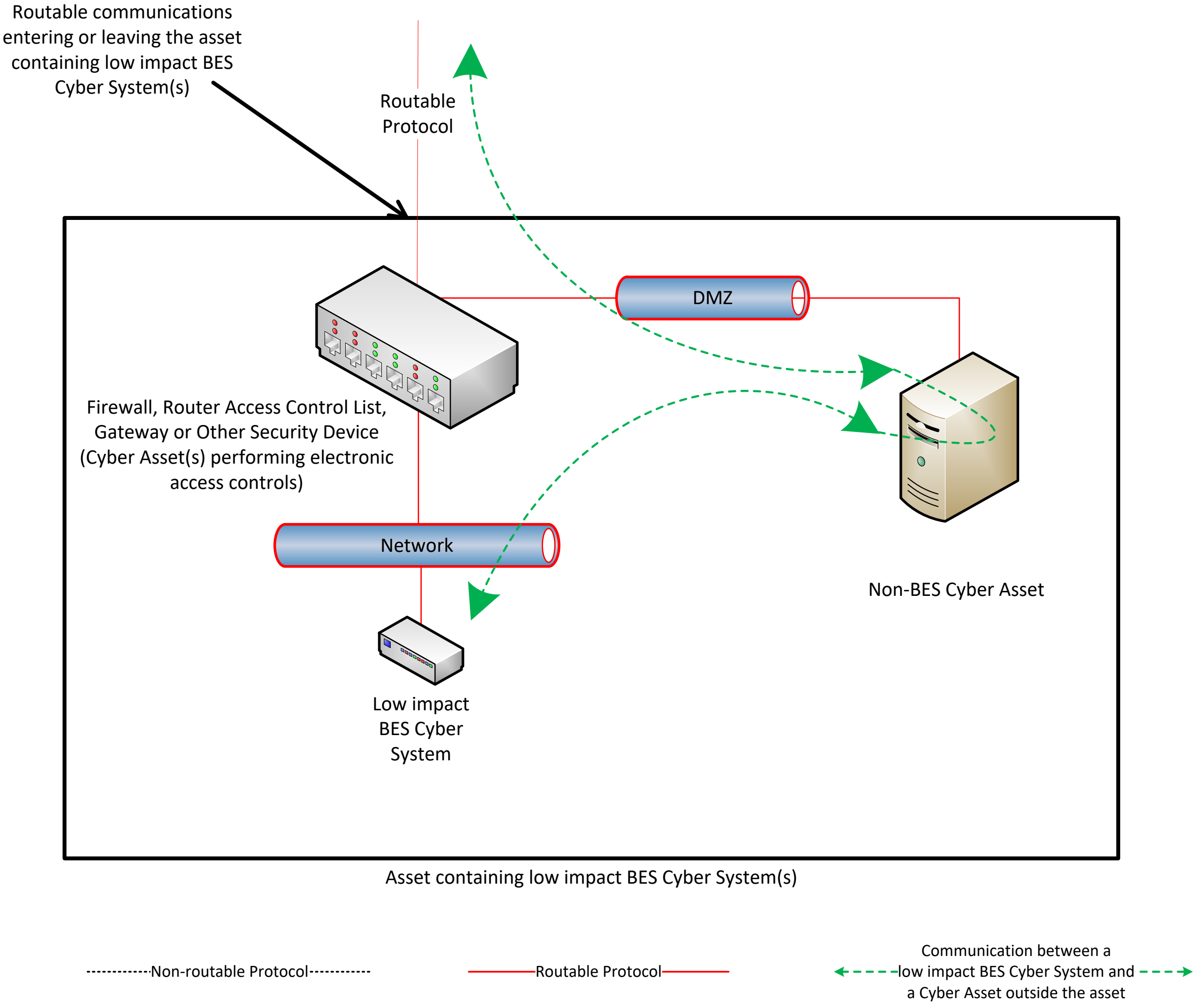
This reference model demonstrates that Responsible Entities have flexibility in choosing electronic access controls so long as the security objective of the requirement is met. The Responsible Entity may choose to utilize a non-BES Cyber Asset located at the asset containing the low impact BES Cyber System that requires authentication for communication from the Cyber Asset(s) outside the asset. This non-BES Cyber System performing the authentication permits only authenticated communication to connect to the low impact BES Cyber System(s), meeting the first half of the security objective to permit only necessary inbound electronic access. Additionally, the non-BES Cyber System performing authentication is configured such that it permits only necessary outbound communication meeting the second half of the security objective. Often, the outbound communications would be controlled in this network architecture by permitting no communication to be initiated from the low impact BES Cyber System. This configuration may be beneficial when the only communication to a device is for user-initiated interactive access.



Reference Model 5

Reference Model 6 – Indirect Access

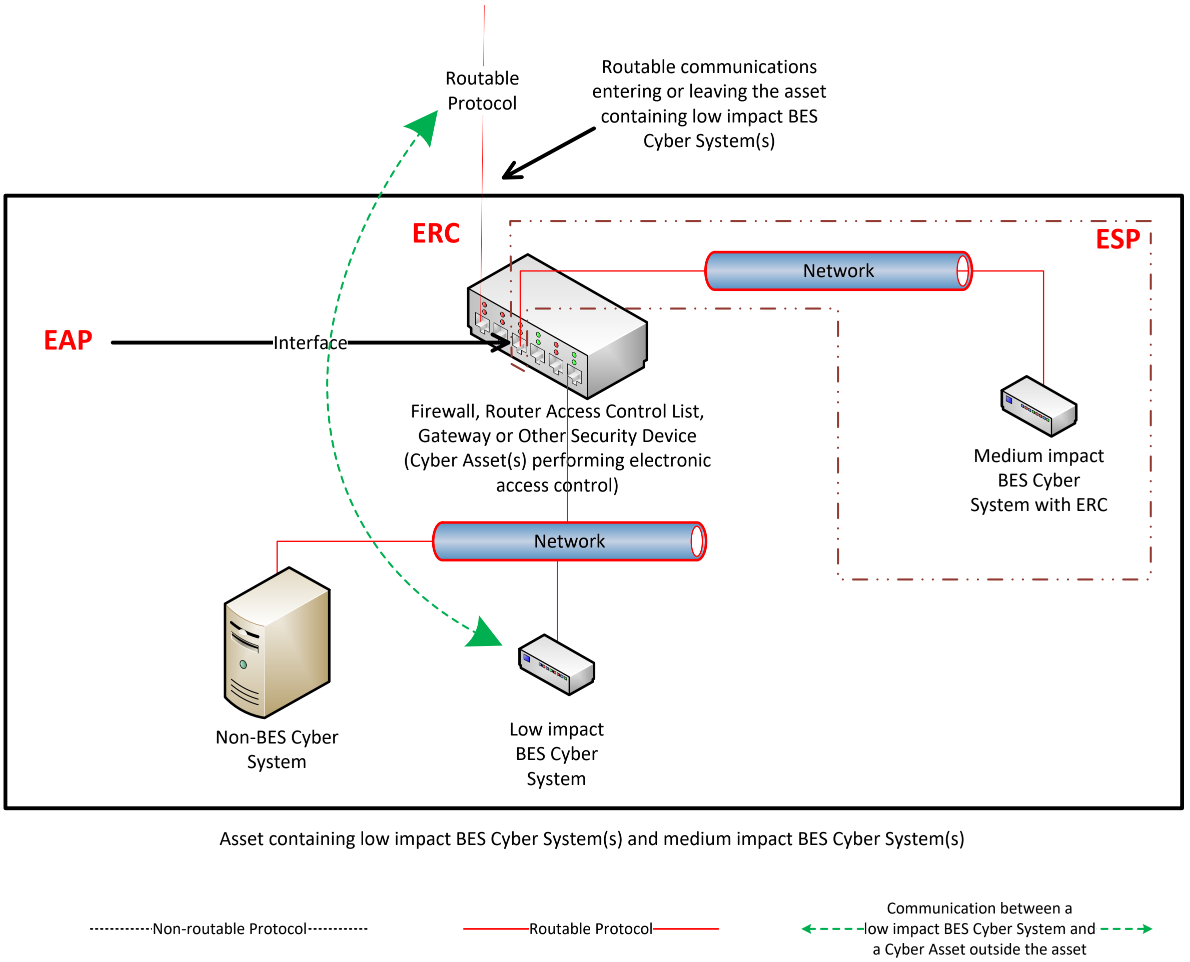
In implementing its electronic access controls, the Responsible Entity may identify that it has indirect access between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System through a non-BES Cyber Asset located within the asset. This indirect access meets the criteria of having communication between the low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System. In this reference model, it is intended that the Responsible Entity implement electronic access controls that permit only necessary inbound and outbound electronic access to the low impact BES Cyber System. Consistent with the other reference models provided, the electronic access in this reference model is controlled using the security device that is restricting the communication that is entering or leaving the asset.



Reference Model 6

Reference Model 7 – Electronic Access Controls at assets containing low impact BES Cyber Systems and ERC

In this reference model, there is both a routable protocol entering and leaving the asset containing the low impact BES Cyber System(s) that is used by Cyber Asset(s) outside the asset and External Routable Connectivity because there is at least one medium impact BES Cyber System and one low impact BES Cyber System within the asset using the routable protocol communications. The Responsible Entity may choose to leverage an interface on the medium impact Electronic Access Control or Monitoring Systems (EACMS) to provide electronic access controls for purposes of CIP-003. The EACMS is therefore performing multiple functions – as a medium impact EACMS and as implementing electronic access controls for an asset containing low impact BES Cyber Systems.



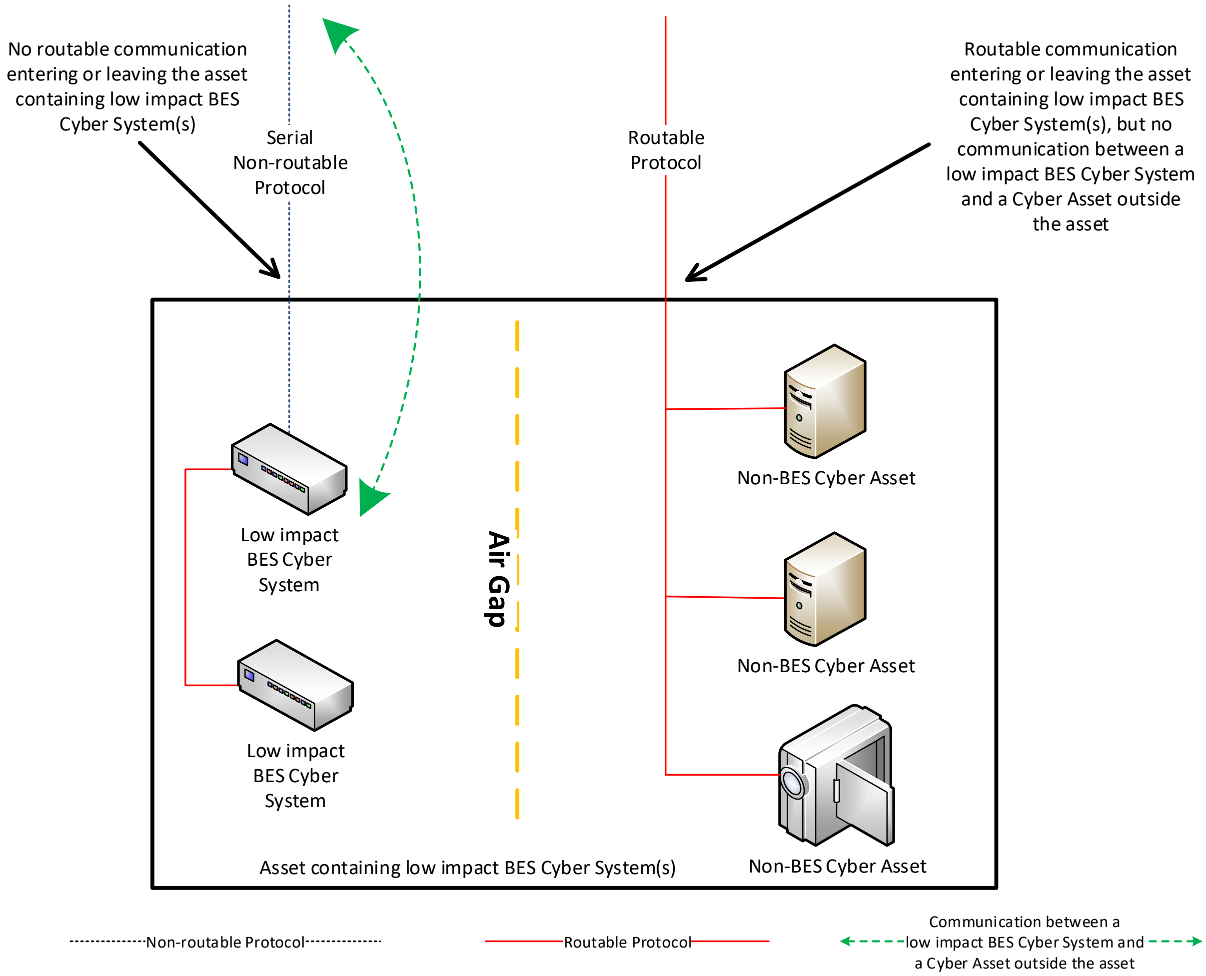
Reference Model 7

Reference Model 8 – Physical Isolation and Serial Non-routable Communications – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model demonstrates three concepts:

1) The physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an 'air gap', mitigates the need to implement the required electronic access controls;
2) The communication to the low impact BES Cyber System from a Cyber Asset outside the asset containing the low impact BES Cyber System(s) using only a serial non-routable protocol where such communication is entering or leaving the asset mitigates the need to implement the required electronic access controls.
3) The routable protocol communication between the low impact BES Cyber System(s) and other Cyber Asset(s), such as the second low impact BES Cyber System depicted, may exist without needing to implement the required electronic access controls so long as the routable protocol communications never leaves the asset containing the low impact BES Cyber System(s).

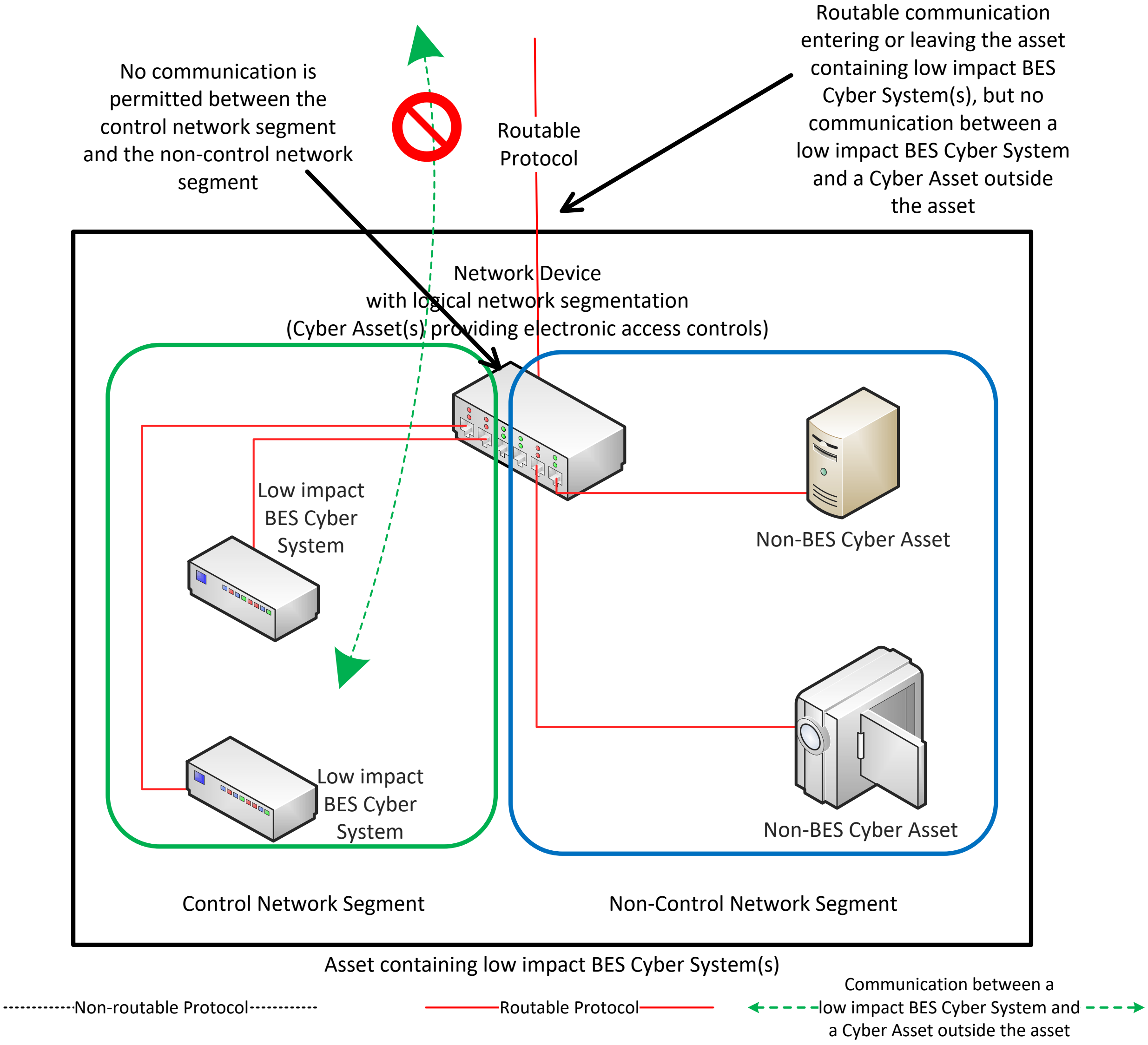
Section 1.



Reference Model 8

Reference Model 9 – Logical Isolation - No Electronic Access Controls Required

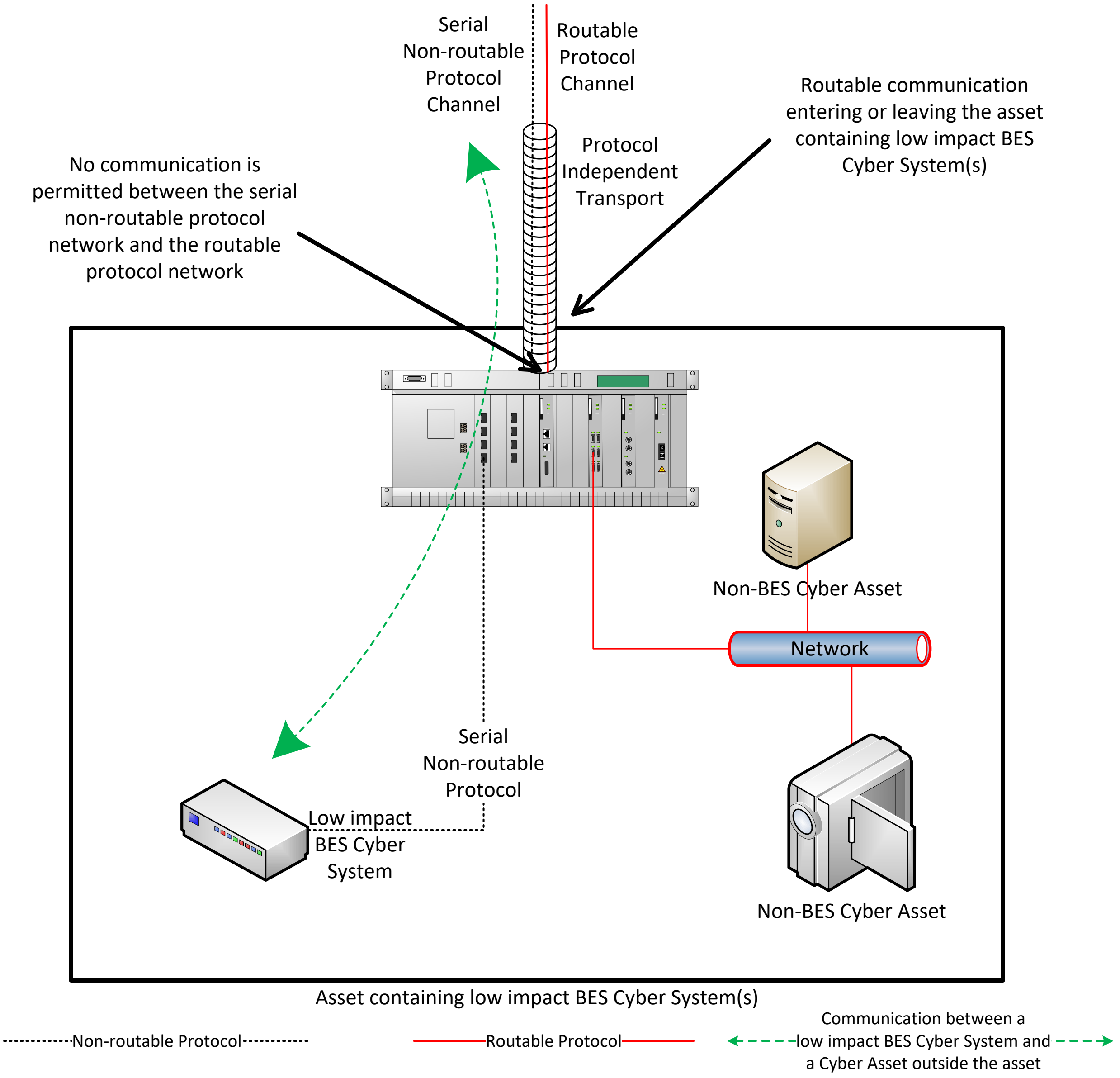
In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. The Responsible Entity has logically isolated the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing low impact BES Cyber System(s). The logical network segmentation in this reference model permits no communication between a low impact BES Cyber System and a Cyber Asset outside the asset. Additionally, no indirect access exists because those non-BES Cyber Assets that are able to communicate outside the asset are strictly prohibited from communicating to the low impact BES Cyber System(s). The low impact BES Cyber System(s) is on an isolated network segment with logical controls preventing routable protocol communication into or out of the network containing the low impact BES Cyber System(s) and these communications never leave the asset using a routable protocol.



Reference Model 9

Reference Model 10 - Serial Non-routable Communications Traversing an Isolated Channel on a Non-routable Transport Network – No Electronic Access Controls Required

In this reference model, the criteria from Attachment 1, Section 3.1 requiring the implementation of electronic access controls are not met. This reference model depicts communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing the low impact BES Cyber System over a serial non-routable protocol which is transported across a wide-area network using a protocol independent transport that may carry routable and non-routable communication such as a Time-Division Multiplexing (TDM) network, a Synchronous Optical Network (SONET), or a Multiprotocol Label Switching (MPLS) network. While there is routable protocol communication entering or leaving the asset containing low impact BES Cyber Systems(s) and there is communication between a low impact BES Cyber System and a Cyber Asset outside the asset, the communication between the low impact BES Cyber System and the Cyber Asset outside the asset is not using the routable protocol communication. This model is related to Reference Model 9 in that it relies on logical isolation to prohibit the communication between a low impact BES Cyber System and a Cyber Asset outside the asset from using a routable protocol.



Reference Model 10

Dial-up Connectivity

Dial-up Connectivity to a low impact BES Cyber System is set to dial out only (no auto-answer) to a preprogrammed number to deliver data. Incoming Dial-up Connectivity is to a dialback modem, a modem that must be remotely controlled by the control center or control room, has some form of access control, or the low impact BES Cyber System has access control.

Insufficient Access Controls

Some examples of situations that would lack sufficient access controls to meet the intent of this requirement include:

- An asset has Dial-up Connectivity and a low impact BES Cyber System is reachable via an auto-answer modem that connects any caller to the Cyber Asset that has a default password. There is no practical access control in this instance.
- A low impact BES Cyber System has a wireless card on a public carrier that allows the BES Cyber System to be reachable via a public IP address. In essence, low impact BES Cyber Systems should not be accessible from the Internet and search engines such as Shodan.
- Dual-homing or multiple-network interface cards without disabling IP forwarding in the non-BES Cyber Asset within the DMZ to provide separation between the low impact BES Cyber System(s) and the external network would not meet the intent of “controlling” inbound and outbound electronic access assuming there was no other host-based firewall or other security devices on the non-BES Cyber Asset.

Requirement R2, Attachment 1, Section 4 – Cyber Security Incident Response

The entity should have one or more documented Cyber Security Incident response plan(s) that include each of the topics listed in Section 4. If, in the normal course of business, suspicious activities are noted at an asset containing low impact BES Cyber System(s), the intent is for the entity to implement a Cyber Security Incident response plan that will guide the entity in responding to the incident and reporting the incident if it rises to the level of a Reportable Cyber Security Incident.

Entities are provided the flexibility to develop their Attachment 1, Section 4 Cyber Security Incident response plan(s) by asset or group of assets. The plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can choose to use a single enterprise-wide plan to fulfill the obligations for low impact BES Cyber Systems.

The plan(s) must be tested once every 36 months. This is not an exercise per low impact BES Cyber Asset or per type of BES Cyber Asset but rather is an exercise of each incident response plan the entity created to meet this requirement. An actual Reportable Cyber Security Incident counts as an exercise as do other forms of tabletop exercises or drills. NERC-led exercises such as GridEx participation would also count as an exercise provided the entity’s response plan is followed. The intent of the requirement is for entities to keep the Cyber Security Incident response plan(s) current, which includes updating the plan(s), if needed, within 180 days following a test or an actual incident.

For low impact BES Cyber Systems, the only portion of the definition of Cyber Security Incident that would apply is, “A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.” The other portion of that definition is not to be used to require ESPs and PSPs for low impact BES Cyber Systems.

Requirement R2, Attachment 1, Section 5 – Transient Cyber Assets and Removable Media Malicious Code Risk Mitigation

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the BES Cyber Assets and BES Cyber Systems, CIP-003 Requirement R2, Attachment 1, Section 5 requires Responsible Entities to document and implement a plan for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to the BES Cyber Asset(s) or BES Cyber System(s). Note: Cyber Assets connected to a BES Cyber System for less than 30 days due to an unplanned removal, such as premature failure, are not intended to be identified as Transient Cyber Assets. Removable Media subject to this requirement include, among others, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Equipment used for BES Cyber System maintenance; or
- Equipment used for BES Cyber System configuration.

To meet the objective of mitigating risks associated with the introduction of malicious code at low impact BES Cyber Systems, Section 5 specifies the capabilities and possible security methods available to Responsible Entities based upon asset type and ownership.

With the list of options provided in Attachment 1, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset or BES Cyber Asset.

Malicious Code Risk Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in Section 5 in Attachment 1 to address the risks posed by malicious code when connecting Transient Cyber Assets and Removable Media to BES Cyber Systems. Mitigation is intended to mean that entities reduce security risks presented by connecting the Transient Cyber Asset or Removable Media. When determining the method(s) to mitigate the introduction of malicious code, it is not intended for entities to perform and document a formal risk assessment associated with the introduction of malicious code.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R2, Attachment 1, Section 5.1 - Transient Cyber Asset(s) Managed by the Responsible Entity

For Transient Cyber Assets and Removable Media that are connected to both low impact and medium/high impact BES Cyber Systems, entities must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

Section 5.1: Entities are to document and implement their plan(s) to mitigate malicious code through the use of one or more of the protective measures listed, based on the capability of the Transient Cyber Asset.

The Responsible Entity has the flexibility to apply the selected method(s) to meet the objective of mitigating the introductions of malicious code either in an on-going or in an on-demand manner. An example of managing a device in an on-going manner is having the antivirus solution for the device managed as part of an end-point security solution with current signature or pattern updates, regularly scheduled systems scans, etc. In contrast, for devices that are used infrequently and the signatures or patterns are not kept current, the entity may manage those devices in an on-demand manner by requiring an update to the signatures or patterns and a scan of the device before the device is connected to ensure that it is free of malicious code.

Selecting management in an on-going or on-demand manner is not intended to imply that the control has to be verified at every single connection. For example, if the device is managed in an on-demand manner, but will be used to perform maintenance on several BES Cyber Asset(s), the Responsible Entity may choose to document that the Transient Cyber Asset has been updated before being connected as a Transient Cyber Asset for the first use of that maintenance work. The intent is not to require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

The following is additional discussion of the methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the BES Cyber Asset or BES Cyber System.
- When using methods other than those listed, entities need to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. An entity may choose to not connect the Transient Cyber Asset to a BES Cyber System to prevent the malicious code from being introduced into the BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

Section 5 also recognizes the lack of direct control over Transient Cyber Assets that are managed by parties other than the Responsible Entity. This lack of control, however, does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to mitigate the introduction of malicious code to low impact BES Cyber System(s) from Transient Cyber Assets it does not manage. Section 5 requires entities to review the other party's security practices with respect to Transient Cyber Assets to help meet the objective of the requirement. The use of "prior to connecting the Transient Cyber Assets" is intended to ensure that the Responsible Entity conducts the review before the first connection of the Transient Cyber Asset to help meet the objective to mitigate the introduction of malicious code. The SDT does not intend for the Responsible Entity to conduct a review for every single connection of that Transient Cyber Asset once the Responsible Entity has established the Transient Cyber Asset is meeting the security objective. The intent is to not require a log documenting each connection of a Transient Cyber Asset to a BES Cyber Asset.

To facilitate these controls, Responsible Entities may execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014.[6] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities may consider the "General Cybersecurity

---

[6] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 5.2.1: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This method intends to reduce the attack surface on the Transient Cyber Asset and reduce the avenues by which malicious software could be introduced.

Section 5.2.2: The intent of this section is to ensure that after conducting the selected review from Section 5.2.1, if there are deficiencies identified, actions mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems must be completed prior to connecting the device(s) to an applicable system.

Requirement R2, Attachment 1, Section 5.3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 5.3: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The SDT does not intend to obligate a Responsible Entity to conduct a review for every single connection of Removable Media, but rather to implement its plan(s) in a manner that protects all BES Cyber Systems where Removable Media may be used. The intent is to not require a log documenting each connection of Removable Media to a BES Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 5.3.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System.

Requirement R3:

The intent of CIP-003-8, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Reliability Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that the CIP Senior Manager will play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-8, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the intent is to afford the Responsible Entity significant flexibility to adapt this requirement to its existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records shows a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up-to-date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or the individual is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

One or more security policies enable effective implementation of the requirements of the cyber security Reliability Standards. The purpose of policies is to provide a management and governance foundation for all requirements that apply to a Responsible Entity's BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the requirements.

Annual review and approval of the cyber security policies ensures that the policies are kept-up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for Requirement R2:

In response to FERC Order No. 791, Requirement R2 requires entities to develop and implement cyber security plans to meet specific security control objectives for assets containing low impact BES Cyber System(s). The cyber security plan(s) covers five subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; (4) Cyber Security Incident response; and (5) Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation. This plan(s), along with the cyber security policies required under Requirement R1, Part 1.2, provides a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Considering the varied types of low impact BES Cyber Systems across the BES, Attachment 1 provides Responsible Entities flexibility on how to apply the security controls to meet the security objectives. Additionally, because many Responsible Entities have multiple-impact rated BES Cyber Systems, nothing in the requirement prohibits entities from using their high and medium impact BES Cyber System policies, procedures, and processes to implement security controls required for low impact BES Cyber Systems, as detailed in Requirement R2, Attachment 1.

Responsible Entities will use their identified assets containing low impact BES Cyber System(s) (developed pursuant to CIP-002) to substantiate the sites or locations associated with low impact BES Cyber System(s). However, there is no requirement or compliance expectation for Responsible Entities to maintain a list(s) of individual low impact BES Cyber System(s) and their associated cyber assets or to maintain a list of authorized users.

Rationale for Modifications to Sections 2 and 3 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 73 of FERC Order No. 822, the Commission directed NERC to modify "…the Low Impact External Routable Connectivity definition to reflect the commentary in the Guidelines and Technical Basis section of CIP-003-6…to provide needed clarity to the definition and eliminate ambiguity surrounding the term 'direct' as it is used in the proposed definition…within one year of the effective date of this Final Rule."

The revisions to Section 3 incorporate select language from the LERC definition into Attachment 1 and focus the requirement on implementing electronic access controls for asset(s) containing low impact BES Cyber System(s). This change requires the Responsible Entity to permit only necessary inbound and outbound electronic access when using a routable protocol entering or leaving the asset between low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber system(s). When this communication is present, Responsible Entities are required to implement electronic access controls unless that communication meets the following exclusion language (previously in the definition of LERC) contained in romanette (iii): "not used for time-sensitive protection or control functions between intelligent electronic devices (e.g. communications using protocol IEC TR-61850-90-5 R-GOOSE)".

The revisions to Section 2 of Attachment 1 complement the revisions to Section 3; consequently, the requirement now mandates the Responsible Entity control physical access to "the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any." The focus on electronic access controls rather than on the Low Impact BES Cyber System Electronic Access Points (LEAPs) eliminates the need for LEAPs.

Given these revisions to Sections 2 and 3, the NERC Glossary terms: Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) will be retired.

Rationale for Section 5 of Attachment 1 (Requirement R2):

Requirement R2 mandates that entities develop and implement one or more cyber security plan(s) to meet specific security objectives for assets containing low impact BES Cyber System(s). In Paragraph 32 of FERC Order No. 822, the Commission directed NERC to "…provide mandatory protection for transient devices used at Low Impact BES Cyber Systems based on the risk posed to bulk electric system reliability." Transient devices are potential vehicles for introducing malicious code into low impact BES Cyber Systems. Section 5 of Attachment 1 is intended to mitigate the risk of malware propagation to the BES through low impact BES Cyber Systems by requiring entities to develop and implement one or more plan(s) to address the risk. The cyber security plan(s) along with the cyber security policies required under Requirement R1, Part 1.2, provide a framework for operational, procedural, and technical safeguards for low impact BES Cyber Systems.

Rationale for Requirement R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the Glossary of Terms used in NERC Reliability Standards so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the CIP Senior Manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for Requirement R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for “clear lines of authority and ownership for security matters.” With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Personnel & Training

Technical Rationale and Justification for Reliability Standard CIP-004-8

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-004-8

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-004-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-004-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the issues identified by the V5TAG was virtualization. The V5TAG Transfer document states, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale." Document for reference when reading the technical rationale that follows.

Requirement R1-R6

General Considerations

For Requirements R2 through R6, the Project 2016-02 SDT added a new type of 'Applicable System' called '**Medium impact BCS with IRA**'. As the SDT is addressing IRA to a non-routable BCA/BCS through scenarios such as IP-to-serial conversion, IRA is no longer dependent on ERC and "associated ESPs". Therefore, CIP-004 requirements for provisioning and deprovisioning IRA for personnel can no longer be limited to only medium impact BCS with ERC.

However, several of the Requirement Parts cover both physical and electronic access and the "with ERC" has been used as a scoping filter so that, for example, you don't have to deprovision physical access within 24 hours at a remote site that has no ERC and changes for physical security may require a site visit. To account for this situation, several of the Requirement Parts now include a "(except for Medium impact BCS without ERC)" exclusion on the physical access portions of the language.

Note that by adding this to Requirement 2, Part 2.1 it does not mean that all personnel who would ONLY need IRA (i.e., vendors with occasional remote access needs) would need training on all content listed. R2 states the training program is “appropriate to individual roles, functions, or responsibilities”.

The Project 2016-02 SDT also made conforming changes to Reliability Standard CIP-004-8 to align personnel and training requirements with the virtualization changes.

To enable CIP-004-8 for virtualization, the SDT added “Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part” within the Applicable Systems column of each of the Parts for Requirement R1 – Requirement R6.

Additionally, where the term BES Cyber System (BCS) was used in the requirement language, it is replaced with “Applicable Systems” to align the requirement language of each Requirement Part with the updated applicability for each Requirement Part.

Requirement R3 Part 3.5

Summary of Changes:

A CIP Exceptional Circumstance was added as an exception to “Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 through 3.4 within the last seven years” such that individuals granted authorized electronic access and authorized unescorted physical access have undergone the personnel risk assessment processes.

Change Rationale:

The SDT determined Responsible Entities cannot require personnel risk assessments for first responders prior to granting them authorized unescorted physical access during certain conditions that qualify as CIP Exceptional Circumstances.

Former Background Section from Reliability Standard CIP-004-7

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-004 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, *"Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference]."* The referenced table requires the applicable items in the procedures for the common subject matter of the requirements.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of documented processes where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as plans (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics.

The following conventions are used in the “Applicable Systems” column as described. High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1a identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-004-7

General Considerations for Requirement R1

None

Rationale for Requirement R1

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table Requirement R2.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets (TCA) and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, TCA and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3

General Considerations for Requirement R3

None

Rationale for Requirement R3

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new personnel risk assessment (PRA). Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4

General Considerations for Requirement R4

None

Rationale for Requirement R4

Authorization for electronic and unescorted physical access must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5

General Considerations for Requirement R5

None

Rationale for Requirement R5

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked.

The initial revocation required in Requirement R5 Part 5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement R5 Part 5.5 specified that passwords for shared account are to be changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the Bulk Electric System. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Requirement R6

General Considerations for Requirement R6

None

Rationale for Requirement R6

Requirement R6 requires Responsible Entities to implement a BES Cyber System Information (BCSI) access management program to ensure that provisioned access to BCSI is authorized, verified, and promptly revoked. Authorization ensures only individuals who have a need are authorized for provisioned access to BCSI. Prompt revocation of terminated individuals’ ability to access BCSI helps prevent inappropriate disclosure or use of BCSI. Periodic verification ensures that what is currently provisioned is authorized and still required, and allows the Responsible Entity the opportunity to correct any errors in provisioning.

The change to “provisioned access” instead of “designated storage locations” enables the use of third-party solutions (e.g., cloud services) for BCSI. The concept of “designated storage locations” is too prescriptive and limiting for entities that want to implement file-level rights and permissions (i.e., policy based credentials or encryption keys that follow the file and the provisioned individual), which provide BCSI access controls regardless of storage location. The concept of provisioned access provides the needed flexibility for entities to use other technologies and approaches instead of or in addition to storage locations as a way to meet the access management requirements for BCSI, especially that which is stored in third-party cloud solutions or is protected at the information/file level no matter where it is located.

According to Requirement R6, Part 6.1, the Responsible Entity must authorize individuals to be given provisioned access to BCSI. First, the Responsible Entity determines who needs the ability to obtain and use BCSI for performing legitimate work functions. Next, a person empowered by the Responsible Entity to do so authorizes—gives permission or approval for—those individuals to be given provisioned access to BCSI. Only then would the Responsible Entity provision access to BCSI as authorized.

Provisioned access is to be considered the result of specific actions taken to provide an individual the means to access BCSI (e.g., physical keys or access cards, user accounts and associated rights and privileges, encryption keys, etc.). In the context of this requirement, an individual is considered to have been provisioned access if they concurrently have the means to both obtain and use the BCSI. To illustrate, an individual who can obtain encrypted BCSI but does not have the encryption keys to be able to use the BCSI has not been provisioned access to the BCSI.

For BCSI in physical format, physical access is provisioned to a physical storage location designated for BCSI and for which access can be provisioned, such as a lockable file cabinet. For BCSI in electronic format, electronic access is provisioned to an electronic system or its contents, or to individual files. Provisioned physical access alone to a physical location housing hardware that contains electronic BCSI is not considered to be provisioned access to the electronic BCSI. Take, for instance, storing BCSI with a cloud service provider. In this case, the cloud service provider’s personnel with physical access to the data center is not, by itself, considered provisioned access to the electronic BCSI stored on servers in that data center, as the personnel would also need to be provisioned electronic access to the servers or system. In scenarios like this, the Responsible Entity should implement appropriate information protection controls to help prevent unauthorized access to BCSI per its information protection program, as required in CIP-011-X. The subparts in Requirement R6, Part 6.1 were written to reinforce this concept and clarify access management requirements.

The periodic verification required by Requirement R6 Part 6.2 is to ensure that only authorized individuals have been provisioned access to BCSI and that what is provisioned is what each individual currently needs to perform work functions. For example, by performing the verification, the Responsible Entity might identify individuals who have changed jobs and no longer have a need for provisioned access to BCSI, and would therefore revoke provisioned access.

For Requirement R6 Part 6.3, removal of an individual’s ability to use provisioned access to BCSI is considered to mean a process with the result that electronic access to electronic BCSI and physical access to physical BCSI is no longer possible from that point in time onwards using the means the individual had been given to obtain and use BCSI in those circumstances. Either what was specifically provisioned to give an individual access to BCSI (e.g., keys, local user or database accounts and associated privileges, etc.) is taken away, deleted, disabled, revoked, etc. (also known as “deprovisioning”), or some primary access is removed which prevents the individual from using the specifically provisioned means. Requirement R6 Part 6.3 acknowledges that where removing unescorted physical access and Interactive Remote Access, such as is required in Requirement R5 Part 5.1, prevents any further access to BCSI by the individual after termination, then this would constitute removal of an individual’s ability to use provisioned access to BCSI. Access can only be revoked or removed where access has been provisioned. The intent is not to have to retrieve individual pieces of BCSI (e.g., documents) that might be in someone’s possession (although you should if you can, but the individual cannot un-see what they have already seen).

Where no specific mechanisms are available or feasible for provisioning access to BCSI, these requirements are not applicable. For example, there is no available or feasible mechanism to provision access in instances when an individual is merely given, views, or might see BCSI, such as when the individual is handed a piece of paper during a meeting or sees a whiteboard in a conference room. Likewise, these requirements are not applicable where provisioned electronic or physical access is not specifically intended to provide an individual the means to obtain and use BCSI. There will likely be no specific provisioning of access to BCSI on workstations, laptops, flash drives, portable equipment, offices, vehicles, etc., especially when BCSI is only temporarily or incidentally located or stored there. Another example is the provisioning of access to a substation, the intent of which is to enable an individual to gain access to the substation to perform substation-related work tasks, not to access BCSI that may be located there. However, BCSI in these locations and situations still needs to be protected against unauthorized access per the Responsible Entity’s information protection program as required by CIP-011-X.

The change to “provisioned access” to BCSI is backwards compatible with the previous “designated storage locations” concept. Entities have likely designated only those storage locations to which access can be provisioned, rather than any location where BCSI might be found. Both concepts intend to exclude those locations where BCSI is temporarily stored, as explained in the previous paragraph. Provisioned access, like designated storage locations, maintains the scope to a finite and discrete object that is manageable and auditable, rather than trying to manage access to individual pieces of information. The removal of the term “designated storage location” does not preclude an entity from defining storage locations for the entity’s access management program for authorization, verification, and revocation of access to BCSI.

Technical Rationale for Reliability Standard CIP-004-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-004-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. Additionally, training should address the risk posed when connecting and using Transient Cyber Assets and Removable Media with BES Cyber Systems or within an Electronic Security Perimeter. As noted in FERC Order No. 791, Paragraph 135, Transient Cyber Assets and Removable Media have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations. Training on their use is a key element in protecting BES Cyber Systems. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role, or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

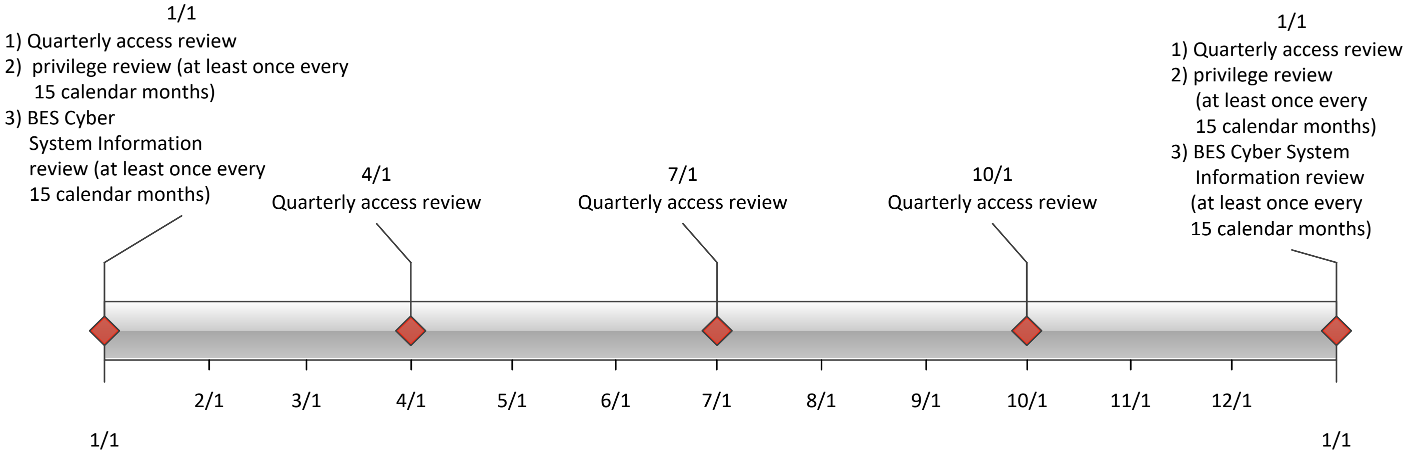
A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.



Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Rationale for Requirement R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Rationale for Requirement R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Rationale for Requirement R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-6. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-6 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Rationale for Requirement R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security – Electronic Security Perimeter(s)

Technical Rationale and Justification for Reliability Standard CIP-005-8

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-005-8

Introduction

This document is the technical rationale and justification for Reliability Standard CIP-005. It includes the rationale for changes in the current proposed version (CIP-005-8) as well as previous versions of the standard. The intent of this document is to provide stakeholders and the ERO Enterprise with an understanding of the revisions and the technical concepts of the Reliability Standard as well as the rationale for such revisions, both the currently proposed and historical revisions from previous versions and SDTs.

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-8. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-8 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition Advisory Group (V5TAG), which consisted of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005-8 and the definitions of Cyber Asset and Electronic Access Point (EAP) that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

Summary

The Project 2016-02 Standard Drafting Team (SDT) proposal accommodates for increasing use of virtualization and other technology innovation. The SDT's purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards, but also to better position the CIP standards to be applicable to additional future technological innovation while, to the extent possible, maintaining backwards compatibility.

CIP-005-8 remains a standard concerned with controlling communications to and from BES Cyber Systems (BCS) by establishing an Electronic Security Perimeter (ESP) with increased security controls for Interactive Remote Access (IRA) and vendor remote access. However, virtualization is enabling models for network security, such as "Zero Trust", that are not network perimeter based. Therefore, in CIP-005-8 the ESP focuses on being a security model rather than a network topology-based perimeter as the only option. Securing the communications to and from BCS is the security objective, but the standard no longer prescribes "where", as in where on a network, the controls must be implemented. Innovations such as Zero Trust models are moving access control from network borders to a session level orientation and eliminating the implicit trust within a local network. Network perimeter-based ESP and EAP implementations remain a valid option and are one method for allowing only necessary communications to the Cyber Systems within the ESP.

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 General Considerations

ESP Redefined

For backwards compatibility purposes, network border-based ESPs and EAPs remain a valid option for controlling the communications to and from BCS. However, virtualization technologies and models such as Zero Trust present equally effective methods that are not network border-based solutions. A Zero Trust model can implement more granular controls throughout a network on a per-access or per-session level.

Shared infrastructure and "Mixed Trust" Risks

For virtualized environments where SCI is used, a risk of side channel attacks exists. Virtualization allows disparate workloads of what could be differing impact to execute on the same CPUs and share the same memory (i.e., RAM). In this case the lower impact systems would become high water marked with the higher impact system through the PCA definition. This would in turn affect what requires protection by any associated ESPs. The risks associated with this scenario is mitigated in CIP-005-8 by either:

- Declaring the VCAs that share CPU or memory or are within the same ESP with a BCS as associated PCAs which will require they meet the security requirements (high water marking) that include 'associated PCAs'; or
- Configuring the virtualization infrastructure to place VCAs of differing impact or trust levels into differing CPU and memory pools and configuring affinity controls to these pools such that hypervisors do not allow workloads in these differing pools to simultaneously exist or execute on the same hypervisor.

Assets with Multiple Classifications (PCA, EACMS, Intermediate System, SCI, etc.)

The definitions created to categorize Cyber Assets have historically included overlap. The definition of PCA was revised to include VCAs that share CPU or memory with a BCS. Additional definitions such as SCI and VCA will add to the possibility of additional instances of assets or systems meeting multiple definitions, such as SCI that are also EACMS.

These definitions are used in both the Applicable Systems column as well as within the requirement language. The fact that one asset or system may meet multiple definitions and therefor have multiple classifications does not pose a significant challenge as long as the Responsible Entity ensures that all requirements that pertain to ANY of the classifications are applied. In other words, if an asset or system meets both the SCI and the EACMS definition, requirements that apply to either categorization are applicable.

Firewall/Router on a Stick

A "firewall on a stick" or "router on a stick" is a reference to a networking design scenario by which a firewall or router has one single physical connection to a switch, but has access to multiple networks and broadcast domains by utilizing logical interfaces in combination with VLANs (Virtual Local Area Networks).

Devices on different VLANs are not able to communicate by default, so the primary purpose of this design is to allow for inter-VLAN routing enabling communication between devices which reside on different VLANs by way of the firewall or router.

As all traffic between these VLANs passes through the firewall or router it is uniquely positioned to restrict access and log traffic flows between devices on different VLANs facilitating compliance and the enforcement of security requirements.

This design allows an entity additional flexibility with respect to the creation of multiple Electronic Security Perimeters while minimizing the cost and number of physical networking devices required to provide proper levels of protection and isolation to each of the created Electronic Security Perimeters.

An entity may select this design to enable further isolation of distinct applications and systems from each other based on the assessed risk that they pose to the BES or to enhance their ability to control access to these systems.

Careful attention should be given to the isolation and access control of management interfaces that support this design as they have the potential to impact multiple Electronic Security Perimeters.

SDWAN

Software-Defined Wide Area Networks (SDWANs) are comprised of an underlay network and an overlay network.

The underlay network is what we traditionally refer to as our Wide Area Networks and is constructed with various telecommunications provider circuits and technologies, including Serial, MPLS, LTE, Cable Modem, DSL, etc.

The overlay network is a virtual network layer created upon the underlay network, generally via encrypted tunnels or other similar mechanisms. An overlay network may utilize one or more underlay networks via load balancing or network policies. The policies governing the overlay network may dictate parameters such as what traffic is permitted, what underlay to utilize based on the application type, what should be utilized as the primary path, and various other parameters.

SDWAN enables the construction of secured and isolated network paths with enhanced management and monitoring capabilities in addition to enabling additional services to and from the SDWAN such as VPN connectivity, firewall services, traffic inspection, and shared gateways.

This technology provides an increased level of control over Wide Area Networks while enhancing visibility, security, and redundancy, all while offering the potential to reduce the costs associated with providing connectivity between an entity's locations and assets.

Figure 1 depicts a typical SD-WAN where encrypted tunnels protect traffic between sites A to C as well as sites B to C.

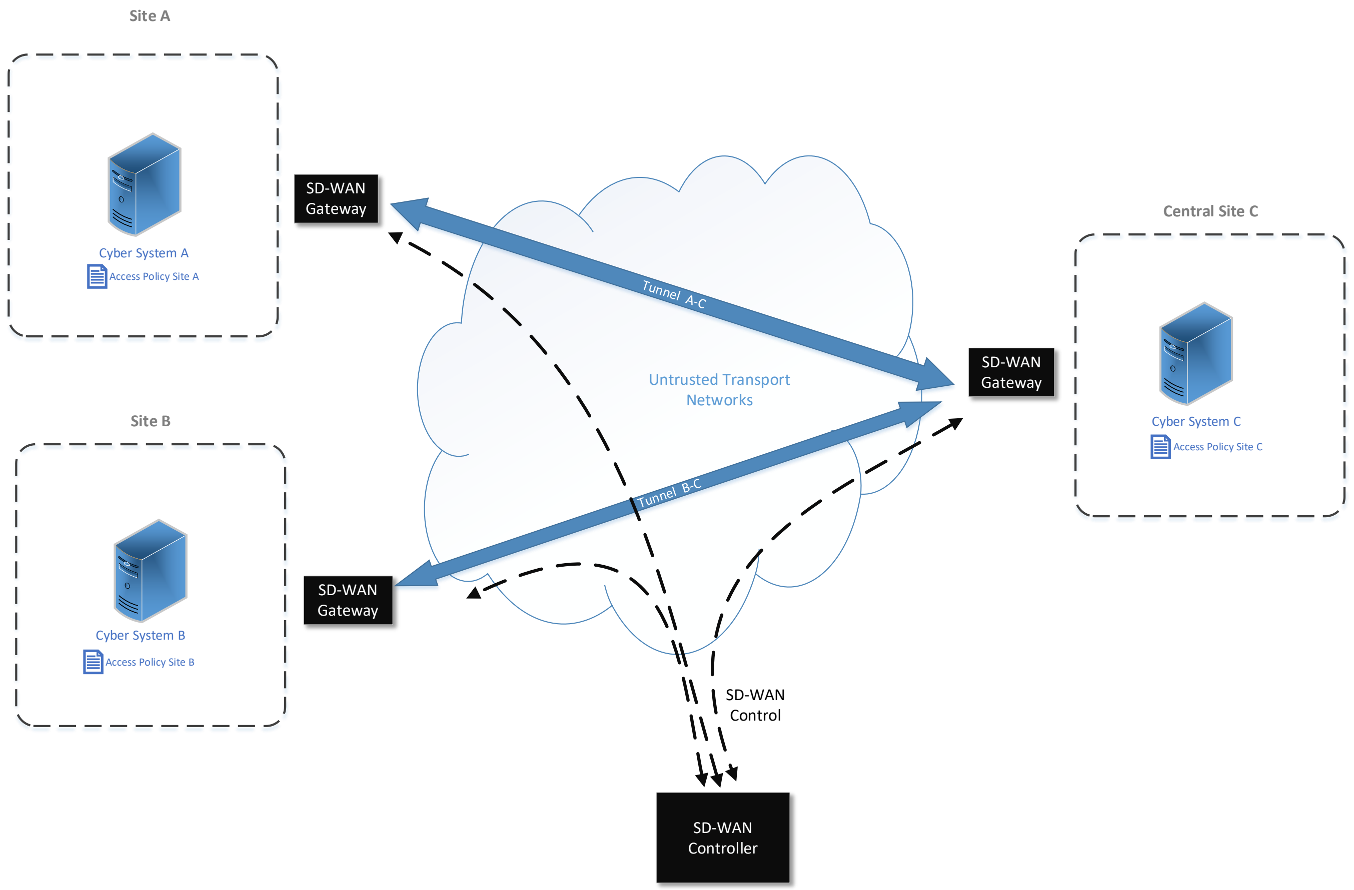


Figure 2 Typical SD-WAN

VXLAN

VXLAN is similar in concept to SDWAN in that it is a form of a Software Defined Network, but in the case of VXLAN the focus is on networks within the Datacenter as opposed to SDWAN which focuses on networks between Datacenters and other facilities.

VXLAN also utilizes the underlay and overlay terminology that we are familiar with given our review of SDWAN. The primary distinction is that VXLAN itself is the name of the overlay protocol utilized in this design and is the most common protocol used for overlay networks within a Datacenter.

The goal of VXLAN is to enhance the ability to segment network resources while also easing the burden of managing, automating, and orchestrating this segmentation by creating a virtual network that is agnostic of the physical network components supporting it.

The VXLAN protocol encapsulates Layer 2 Ethernet frames within Layer 3 UDP packets between devices comprising the design and allows for upwards of 16 million network segments to be created versus the traditional limit of 4094 VLANs. These network segments are identified with a VNI (VXLAN Network Identifier) which is synonymous with VLAN ID.

The components of the design that are capable of encapsulating and de-encapsulating the VXLAN protocol are referred to as VTEPs (VXLAN Tunnel Endpoints) and are commonly network switches or virtual machine hypervisors.

Physical devices and servers rely on switches to act as their VTEP whereas a virtual machine, hosted on VMWare ESX in this example, relies on the hypervisor as its' VTEP.

Figure 3 depicts a typical VXLAN where access control policies are implemented in the IP fabric.

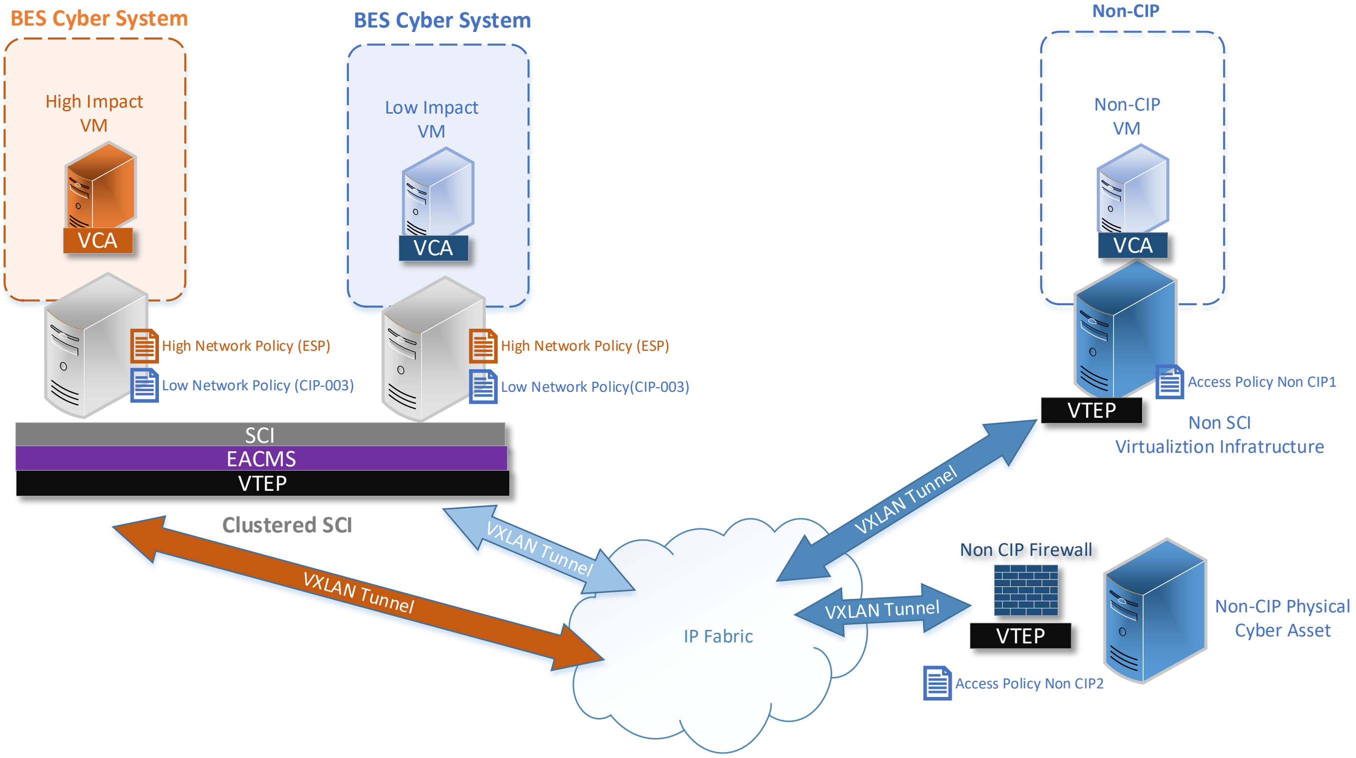


Figure 4 Typical VXLAN

VXLAN facilitates increasing the level of network segmentation within and between an entities Datacenters, while also enhancing their ability to automate and orchestrate the deployment of network resources. With this increased network segmentation an entity is granted more granular control over the flow of traffic and is given more opportunities to inspect that traffic to ensure appropriate levels of access control and protection.

Requirement R1

Rationale

Requirement R1 requires implementation of an ESP for BCS permitting only necessary communication through the ESP. However, there are other network security models available (such as zero trust) that can accomplish this security objective by controlling communications end-to-end at a more granular level than a network perimeter-based model. The definitions (ESP and EAP) and the changes to R1 allow entities the flexibility to implement different models that meet the security objective, or retain their current perimeter-based implementation.

Requirement R1 Part 1.1:

Rationale

This Requirement Part requires all high and medium impact BCS and their associated PCAs to be protected by an ESP. In recognition of non-perimeter based models, the language changed from “shall reside within” to “must be protected by”. Note, a PCA can now be defined by two different attributes of what they share with a BCS – not only network location, but also the sharing of CPU and memory from the underlying hypervisor(s) for VCAs. In the instance

that a VCA becomes an ‘associated PCA’ from its sharing of CPU or memory with a high or medium impact BCS, that associated PCA must also be protected by an ESP.

Note that this Requirement Part applies to all high and medium impact BCS without regard to external connectivity from the local network to other networks. This allows for the identification of PCAs and the scope of TCA connectivity even on isolated networks.

Requirement R1 Part 1.2:

Rationale

This Requirement Part changed to a security objective, rather than prescribing ERC must be controlled at an EAP. Virtualization technologies introduce additional methods to isolate systems. This requirement part no longer prescribes one method of controlling communications to Applicable Systems, and opens it up for alternative solutions.

This allows for other models such as zero trust architectures. Such models are not based on controlling communications at a Cyber Asset interface located on a network boundary. Communications can be authorized by software defined policy enforcement points throughout the infrastructure. In this model, network security is less topology-based and more policy-based (configurations and settings) and can be used to granularly protect communication at an individual system or even process or resource level.

While pure zero-trust architectures are an emerging model, the objective-based requirement also allows for hybrid models of various combinations of network border-based and zero trust architectures. As technology changes, this requirement and broadened ESP definition are flexible in how the objective is met.

The intent of “through the ESP” is to better incorporate future Zero Trust implementations where there is no “logical border surrounding a network” but instead Policy Enforcement Points at the accessed resource itself or as close to it as possible. In these instances that are designed to be perimeter-less, the concepts of “inside” and “outside” begin to fail and the SDT is removing those now to be better prepared for future technologies. The SDT asserts that even in traditional Layer 3 firewalls that define an ESP, the communications between systems that are encapsulated in packets go “through” the perimeter (ESP) in order to reach their destination.

The core security objective, of permitting only needed communications and denying all others by no longer prescribing this must be implemented at a Cyber Asset interface on a network border (an EAP), is retained. The intent of this Requirement Part is to control the ‘reachability’ of the Applicable Systems; filtering network communications *before* they reach the Applicable Systems and their OS, not as part of it. This is not to discourage the use of integrated host-based firewalls to further filter network traffic to a host.

Note that the requirement now explicitly includes “the reason for granting access”. Previously, this had been an implied part of the requirement based on the Measures.

The SDT had considered adding “physical isolation” to the Measure, but did not do so as the applicability explicitly includes ERC. Additionally, within the Measures, the SDT uses examples of VLAN and VXLAN configurations as evidence. These configurations could be used as methods to “Permit only needed routable protocol communications”, despite not being OSI layer routable protocols in and of themselves.

Time-sensitive communications between Protection Systems (i.e., digital relays) that use routable communication protocols are excluded. Time-sensitive in this context generally means functions that would be negatively impacted by the latency introduced in the communications by inserting an ESP and its controls. This time-sensitivity exclusion does not apply to SCADA communications which typically operate on scan rates of 2 seconds or greater. While technically time-sensitive, SCADA communications over routable protocols can withstand the delay introduced by electronic access controls. Examples of excluded time-sensitive communications are those communications which may necessitate the tripping of a breaker within a few cycles (sub-second response times) to protect BES assets. The SDT intent is a Responsible Entity using this technology is not expected to implement the electronic access controls in a situation where it would prohibit the proper function in the proper timeframe.

Requirement R1 Part 1.3:

Rationale

It is important to note that Requirement Part 1.2 is scoped to the Applicable Systems protected by (inside) the ESP while Requirement Part 1.3 is scoped to protect the Management Interface of the Cyber Assets creating and controlling the ESP and thus not protected by the ESP itself. These different scopes show the need for separate Requirements Parts. In addition, the separation into different Requirement Parts prevents a recursive requirement. Otherwise, each EACMS would require an EACMS creating an impossibility to implement.

The objective of this new Requirement Part is to protect ESP configurations and SCI configurations. The intent is preventing unauthorized changes to these important configurations by controlling what can connect to administrative interfaces for SCI and certain EACMS.

This can be done by permitting only needed communications to the Management Interfaces, denying all other communications, of the systems that are providing protection of BCS; namely SCI that is supporting an Applicable System from Part 1.1 (SCI isolates systems of different impact levels from each other) and certain EACMS that are controlling an ESP. This Requirement Part only applies to SCI and EACMS controlling an ESP, and not to the BCS itself).

These are vital controls performing the isolation/segmentation between systems of differing impact levels, and warrant protection of the Management Interface that could be used to compromise them.

Certain EACMS that can control access to an ESP are subject to this requirement. This includes those EACMS such as a firewall that is controlling an ESP, a centralized station administering firewalls controlling ESPs as well as a network switch configured with VLANs to isolate and segment traffic. These certain EACMS will need to have their Management Interfaces protected. The SDT intended to exclude EACMS not associated with control and ESP such as domain controllers that provide only authentication services. The SDT is aware of possible implementations where an authentication server is used to provide real-time control of ESP access on a per user basis. In these situations, the authentication server does fall within scope of an EACMS that controls access to an ESP.

The ‘per system capability’ is included in this Part in recognition that some Management Interfaces, such as “ILO” interfaces, may do inbound but not outbound traffic controls.

Requirement R1 Part 1.4:

Rationale

The SDT included “SCI supporting an Applicable System in this Part” to the scope of the requirement part to ensure that controls regarding Dial-up Connectivity are also applicable to VCAs and SCI; and ‘technical feasibility’ has been replaced with the ‘per system capability’.

Additionally, in order to maintain a decipherable Applicable Systems column, the SDT replaced the scoping phrase “with Dial-Up Connectivity” from the Applicable Systems column, with a reference to “if any” in the Requirement Language.

Requirement R1 Part 1.5:

Rationale

Known or suspected malicious communication detection is specific to routable protocol based traffic that enters or leaves the required ESP. Products available to implement this malicious communication detection are usually based on IP traffic (as defined in RFC 791 and upon which TCP and UDP reside). The SDT intended to exclude other data center communications protocols currently in use such as Fibre Channel, where it would not be possible to meet this requirement.

The requirement applicability was changed to the ESP instead of EAPs; lifting it to an objective level and keeping it from being a prescriptive ‘where’ that forces certain architecture. These protections at the ESP level do not preclude entities from accomplishing the security objective by implementing controls at the EAP level, but offer entities the flexibility to implement other methods at the ESP level.

The SDT considered adding SCI to the Applicable Systems; however, chose not to do so as this functionally may be provided by SCI, thus resulting in a recursive requirement issue. Note that the Management Interfaces of SCI are protected by Requirement R1.3. Entities may wish to implement malicious communications detection on these Management Interfaces of SCI.

Requirement R1 Part 1.6:

Rationale

Requirement R1 Part 1.6 was written to address the issue of “Super ESPs” with high or medium impact BCS at Control Centers that extend a single ESP beyond one PSP. This often applies to virtualized Control Center environments that implement network adjacency to allow workloads to automatically move from one physical location to another to increase BCS resiliency between primary and backup Control Centers.

The security objective is to protect the confidentiality and integrity of the data traversing communication links used to span a single ESP between multiple PSPs. This is especially important when portions of the transport are not within the Registered Entity’s control. Many encryption methods (such as IPSec and TLS) can fulfil this objective; however, some encryption methods fall short of providing both confidentiality and integrity controls.

This Requirement Part works in conjunction with the new 4.2.3.3 exemption in the CIP standards that exempts the Cyber Systems associated with such communication links since the data is required to be protected per this requirement. Also, the former CIP-006-6, Requirement R1, Part 1.10 has been removed and incorporated into this new 1.6 requirement part; consolidating the protections of an ESP and its components that extend outside of a PSP within one standard.

Communications equipment associated with communications links (e.g., equipment belonging to carriers) is exempted from the CIP standards with the 4.2.3.2 exemption. However that only applies to equipment between discrete ESPs. In this extended ESP situation where a single ESP spans multiple sites or PSPs, that exemption does not apply and the potential exists for data to traverse a connection that uses third-party communications equipment that is unprotected inside an ESP; hence the need to enforce confidentiality and integrity controls (such as encryption) on the data that traverses PSPs while within the same ESP to isolate any protected data from access through the communications equipment.

This consolidation also incorporates cabling and non-programmable communication components that are not PSP-protected, intending to protect data moving across the state as well as data traversing cabling that crosses the hall outside of the PSP. Note: the language specifically exempts the data that falls under CIP-012 Requirements in order to avoid the potential for double jeopardy as well as the time-sensitive protection or control functions as described in CIP-005-8 Requirement R1 Part 1.1 above.

The SDT had considered adding SCI to the Applicable Systems; however, chose not to do so as this functionality may be provided by SCI, thus resulting in a “hall of mirrors” issue.

Requirement R2:

General Considerations for Requirement R2.

External Routable Connectivity (ERC) and Interactive Remote Access (IRA)

The ERC and IRA definitions have been updated in order to:

1. Incorporate new models such as Zero Trust where a security perimeter is not necessarily a network perimeter and ESPs become very granular based on policies that can be established at “people to resource” levels rather than IP address levels.
2. Recognize those Cyber Systems that are of an increased risk due to their “reachability” via ERC and that have IRA available to them even if they are serial-only, non-routable devices.
3. Continue to limit scope of Requirement Parts to BCS with ERC and not those that have connectivity such as non-routable serial leased circuits.

The V5TAG transfer document in the SDT’s scope includes the issue of a BES Cyber Asset (BCA) that only uses non-routable protocols over a serial port. These BCAs are not connected to a network with a routable protocol themselves and therefore can be considered to not be within an ESP and thus not have ERC. However, these BCAs can have interactive user access using those serial connections. The SDT’s intent is to clarify that IRA can occur to a device with only a serial, non-routable connection through IP-to-serial conversions and be subject to CIP-005-8 Requirement R2. For example, the intent is to clearly cover situations where a serial-only, non-routable BCA, such as a digital relay in a substation, has its serial communication from a ‘console port’ converted to IP or other routable protocols thus allowing IRA from users outside the substation to use a routable protocol to interact with the serial device and to require the CIP-005-8 Requirement R2 protection for that IRA.

Due to the inclusion of serial based connections into the revised definition of IRA, other CIP requirements (i.e., CIP-004) have been revised to conform. Entities should review serial/IP converters that are currently being used for remote access.

The SDT removed the requirement-style language “The Intermediate System must not be located inside the Electronic Security Perimeter” from the Intermediate System definition in favor of a clarified objective in CIP-005-8 Requirement R2 that all IRA must be *through* an Intermediate System. Requirement R2 Part 2.6 was added to objectively address the location of the Intermediate System.

See the “*CIP Definitions and Exemptions Technical Rationale*” document for further explanation of the changes to the R2 related definitions.

Requirement R2 Part 2.1:

Rationale

Applicable Systems was updated to include SCI to ensure the same safeguards for remote access methods exist for SCI supporting an Applicable System within the Part as they do for the high and medium impact BCS and associated PCA hosted on that SCI. Backwards compatibility is retained for entities that do not use SCI. Please note that there may be situations where an Intermediate System is implemented as a VCA on SCI. The SDT intends that applicability for SCI is to ensure that the objectives of Requirement R1.3 are met such that the Management Interfaces of SCI are appropriately protected. VCAs are not considered part of SCI and therefore could be used to access a Management Interface of SCI.

The requirement language was simplified, and definitions for IRA and Intermediate System have been updated. Please note that the definition of IRA was changed to include serial communications that are converted to/from routable protocols by the Responsible Entity. This change maintains backwards compatibility except where serial connectivity and routable protocol conversion is being used for IRA.

Requirement R2 Part 2.2:

Rationale

The “Applicable Systems” scope was changed to “Intermediate Systems used to access Applicable Systems in Part 2.1”. This clarifies this requirement is associated with the IRA communications between an Intermediate System and the remote clients, as opposed to between the Intermediate System and the BCS. This is important so that it does not require encryption through the ESP to the BCS which would hinder monitoring and inspection.

The requirement was changed from a specific technical-based requirement for encryption to an objective-based requirement to protect confidentiality and integrity of the IRA session between the Intermediate System and the remote client (with encryption as a primary example). The proposed language accounts for the possibility that other equally effective methods could be developed and deployed. This objective also keeps methods from being used that are merely obfuscation methods (XOR, ROT13, etc.) or deprecated encryption methods (DES with 56-bit keys) that no longer meet the objective to protect the confidentiality and integrity of the IRA session.

The changed requirement is backwards compatible except where deprecated encryption methods are in use.

Requirement R2 Part 2.3:

Rationale

Applicable Systems was changed to “Intermediate Systems used to access Applicable Systems of Part 2.1”. This clarifies this requirement is associated with the Intermediate System itself, and where the requirement for multifactor authentication should be applied (multi-factor authentication to the Intermediate System).

Note that the wording of the requirement was updated to specially apply to IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System. This was previously implied.

Requirement R2 Part 2.4 – 2.5:

Rationale

The applicability and requirements have not changed.

Requirement R2 Part 2.6:

Rationale

This is a new requirement that applies to Intermediate Systems. The intent of this new requirement is to further protect the BCS from the Intermediate System by reducing the attack surface between the two. It is important to note that a virtualized Intermediate System (VCA) hosted in such a way that it can share CPU and share memory with a BCS will also meet the definition of PCA and become an ‘associated PCA’ of the BCS. CIP-005 R1.1 requires that PCA to be within an ESP, in conflict with this requirement. This is by design, and thus a VCA performing the function of an Intermediate System must not share CPU or memory with the BCS it is controlling access for. This is due to the access granted to the less trusted side of the Intermediate System and the risk for side-channel attacks to other VCAs sharing the same CPU and memory. Entities must therefore use affinity rules or some other means to keep Intermediate System VCAs from sharing the same CPU and memory as a BCS or its associated PCAs.

Figure 5 depicts an Intermediate System VCA where an affinity ruleset prevents the sharing of CPU or the sharing of memory with a BES System by ensuring these systems run on different on the hypervisor.

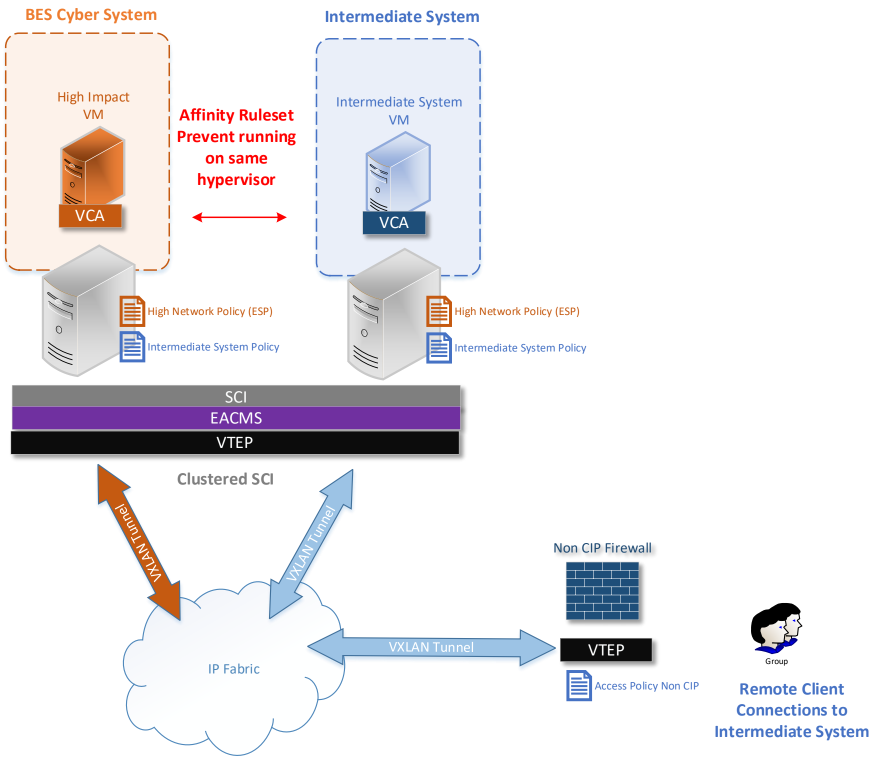


Figure 6 Affinity Rules - Intermediate System does not share CPU or share memory with BES Cyber Systems

Requirement R2 Part 2.7:

Rationale

This is a new requirement that applies to Intermediate Systems. The intent of this new requirement is to further protect the BCS from the Intermediate System by reducing the attack surface between the two. Intermediate Systems have an externally accessible interface that may be used by external parties such as vendors or entity support staff using IRA across an Internet connection to support a remote site. Since Intermediate Systems by nature provide IRA from a less-trusted network and are accessible from yet-to-be authenticated users (in order to authenticate them), a degree of separation from the higher-trust systems they are protecting is necessary in case the Intermediate System is compromised. Previously, this risk was addressed within the glossary definition of Intermediate System ("…must not be located inside the ESP") instead of within an actual requirement. The SDT removed this from the definition and included a security objective in CIP-005-8 Requirement R2 Part 2.7 to require that routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.

It is important to note that the SDT does not intend to prescribe architecture to the point of what Cyber Asset or Virtual Cyber Asset a function may reside. For example, some "security appliances" that have firewall/EAP capability also have separate functionality within them that can perform part of the Intermediate System function. Historically this definition has stated "must not be located inside" which allowed for "outside or ON" the ESP. The SDT does not want to preclude architectures where at least some portion of the Intermediate System functionality may execute on the EAP.

Figure 7 depicts an Intermediate System running on non SCI infrastructure. Network connections from the Intermediate System to the BES Cyber Systems must pass through the ESP protecting those systems. In this case, access control policies, implemented on SCI are used to control network connections.

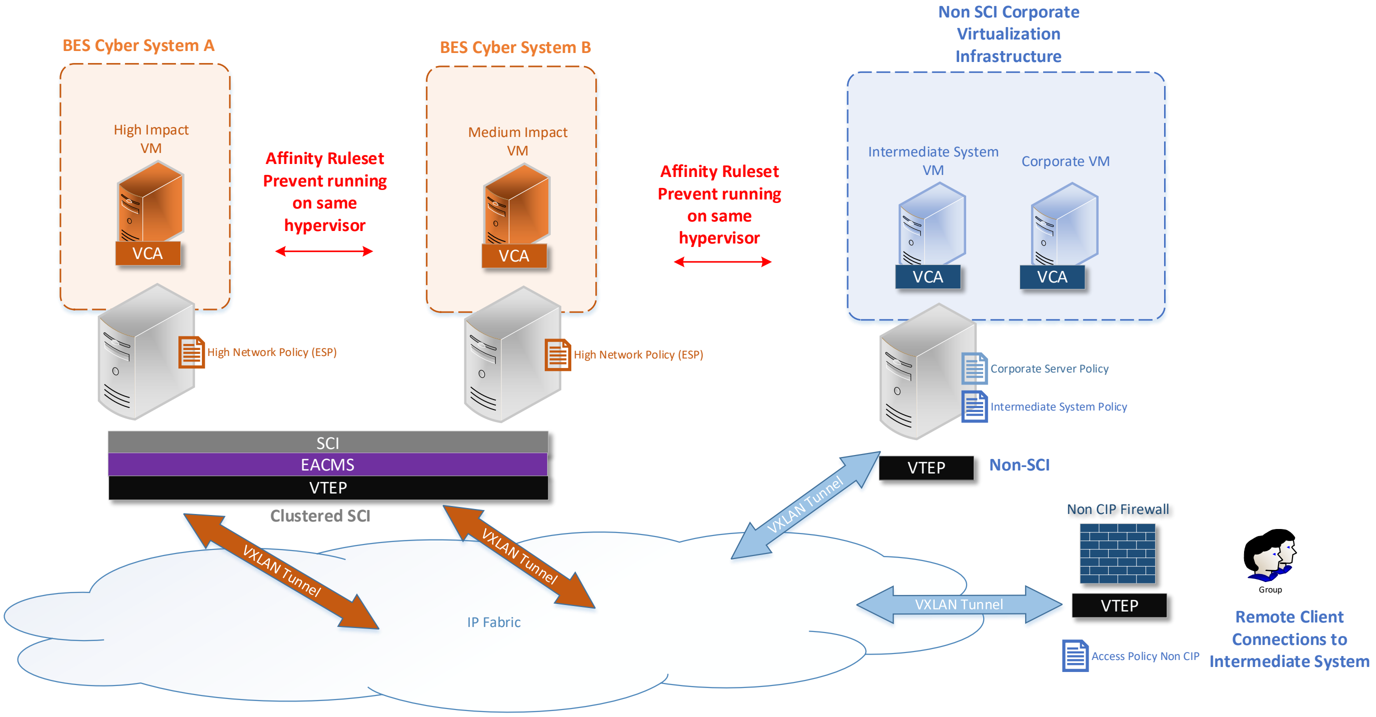


Figure 8 Intermediate System must connect through the Electronic Security Perimeter protecting the BES Cyber Systems

Requirement R3

Rationale

The Applicable Systems section of CIP-005-8 Requirement R3 was updated to include SCI to ensure the same safeguards for vendor-initiated remote connections exist for the applicable SCI. Backwards compatibility is retained for entities that do not currently use SCI.

Background Section from Reliability Standard CIP-005-7

The section 6. Background has been retired. removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BCS and require a minimum level of organizational, operational and procedural controls to mitigate risk to BCS.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BCS. For example, a single training program could meet the requirements for training personnel across multiple BCS.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.

- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

Technical Rationale for Reliability Standard CIP-005-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-005-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-005-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in this Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of Bulk Electric System (BES) Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Updates to this document now include the Project 2019-03 – Cyber Security Supply Chain Risks Standard Drafting Team’s (SDT’s) intent in drafting changes to the requirements.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those system that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-005-7 to require Responsible Entities to meet the directives set forth in the Commission’s Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

Additionally, the Project 2019-03 SDT removed Interchange Coordinator or Interchange Authority as that registration has been retired.

New and Modified Terms Used in NERC Reliability Standards

CIP-005-7 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

The ESP serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network-based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R1

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, then each Cyber Asset of the low impact BES Cyber System are "Associated Protected Cyber Assets" of the high impact BES Cyber System and must meet all the requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero-day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communication to that known range. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rouge connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2

General Considerations for Requirement R2

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources should only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.

But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Requirement R3

Requirement Part 3.1 and Part 3.2 Vendor Remote Access Management for EACMS and PACS

The 2019-03 SDT added Requirement R3 to contain the requirements for all types of vendor remote access management for EACMS and PACS (i.e., system to system, user to system). EACMS were added based on FERC order 850 paragraph 5 where FERC ordered NERC to create a drafting team to add these devices. EACMS were added based on the risks FERC noted in paragraph 4, where a Department of Homeland Security Industrial Control System-Cyber Emergency Response Team (DHS ICS-CERT) said firewalls (normally defined as an EACMS) is the “first line of defense within an Industry Control System (ICS) network environment”. The compromise of those devices that control access management could provide an outsider the “keys to the front door” of the ESP where BES Cyber Systems reside. An intruder holding the “keys to the front door” could use those “keys” to enter the ESP or modify the access controls to allow others to bypass authorization.

In Requirement R3 Part 3.1 and Part 3.2, the word "connection" is the mechanism for a user or a system to interact with an EAMCS or PACS for the purpose of authenticating.

In Requirement R3 Part 3.1 and Part 3.2, the word "authenticate" is the mechanism for the EACMS or PACS to identify the user or device. This permits the EACMS or PACS to first perform its function to authenticate the user or device that is connecting, which in turn permits the entity to delineate or differentiate vendor-initiated connections from other remote access connections. This new proposed language is not prescriptive as to how authentication must occur to permit administrative and technical methods.

In Requirement R3 Part 3.2, the word "control" provides the entity flexibility to allow the vendor to reconnect under a specific set of conditions, established by the entity, where the reconnection is necessary to support critical operations of the entity. If the entity determines that they do not want to allow or does not need to allow a reconnection they can employ means to stop any reconnection.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability

Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Since remotely compromised PACS still require physical presence to exploit BES Cyber Systems, the SDT conducted extensive dialogue and considerations for the addition of PACS. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warranted their inclusion as an applicable Cyber Asset. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[1].

NERC's final report on "*Cyber Security Supply Chain Risks"*, states on page 4, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." PACS are intended to manage physical threats to BES Cyber Systems, thus protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical accesses or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access.

While other Reliability Standards mitigate certain security risks relating to PACS none address supply chain risk. Based on this analysis the SDT included PACS within the applicable section of both Requirement Parts 3.1 and 3.2.

An additional aspect of the NERC Supply Chain Report, the SDT considered was the risk associated with the access control vs. access monitoring functions of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the access control function beyond the access monitoring function. The SDT considered limiting the scope of the requirements to only those access control functions, however chose to stay with the currently approved definition of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally, an attempt to change the EACMS and PACS definition was outside the 2019-03 SAR.

Entities may or may not allow remote access into any of its systems, (BES Cyber Systems, EACMS or PACS), however if remote access is allowed, options to determine remote access connection(s) and capability to disable remote access connection(s) is required.

---

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Technical Rational for Reliability Standard CIP-005-6

This section contains an as-is "cut and paste" of the former Guidelines and Technical Basis (GTB) from Reliability Standard CIP-005-6 Technical Rationale to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Furthermore, Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an “Associated Protected Cyber Asset” of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP.

Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually ‘command and control’ hosts on the Internet, or compromised ‘jump hosts’ within the Responsible Entity’s other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT’s intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity’s address space. The SDT’s intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and ‘deny by default’ type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear ‘perimeter type’ security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions (“TFEs”) rather than increased security.

As for dial-up connectivity, the Standard Drafting Team’s intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords.

But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)

This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Change Rationale: (Part 2.4 and 2.5)
Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Physical Security of BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-006-7

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-006-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-006-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-006-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-006-7 to shorten applicability statements within the body of CIP standards by replacing some terms with the defined acronym for that term:

"BCS" has replaced "BES Cyber System".

"ERC" has replaced "External Routable Connectivity".

"PSP" has replaced "Physical Security Perimeter".

"PACS" has replaced "Physical Access Control Systems".

Requirement R1

Rationale

The SDT made conforming changes to Applicable Systems for virtualization such that protections must be afforded to SCI for relevant Requirement Parts.

Applicable Systems:
Requirement R1 Part 1.1-1.9: the SDT added "SCI supporting an Applicable System in this Part.

Per System Capability vs Technical Feasibility:
Requirement R1 Part 1.3: The SDT chose to remove the reliance on a Technical Feasibility Exception in favor of the updated term "per system capability."

Consolidation:
Requirement R1 Part 1.10: The SDT deleted Requirement R1 Part 1.10 from CIP-006-7 because requirements to protect the data traversing communication links used to span a single ESP between PSPs is incorporated into CIP-005-8 Requirement R1 Part 1.6.

Requirement R2

Rationale

The SDT has include the CIP Exceptional Circumstances within the main R2 requirement text so that it applies to all requirement parts.

The SDT made conforming changes to Applicable Systems for virtualization such that protections must be afforded to SCI for relevant Requirement Parts.

Applicable Systems:
Requirement R2 Part 2.1-2.3: the SDT added "SCI supporting an Applicable System in this Part"

Former Background Section from Reliability Standard CIP-006-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-006 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-006-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-006-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus of this Reliability Standard has shifted away from the definition and management of a completely enclosed "six-wall" boundary, it is expected that in many instances a six-wall boundary will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls outlined below will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access into the PSP.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A logbook or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more PSPs, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, controls for a sole perimeter could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person the guard is observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System, but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

The new requirement part CIP-006-6, Requirement R1, Part 1.10 responds to the directive found in FERC Order No. 791, Paragraph 150. The requirement intends to protect cabling and nonprogrammable communication components that are within an ESP, but extend outside of a PSP. This protection, similar to the FERC Approved NERC Petition on the interpretation on CIP-006-2 from PacifiCorp, must be accomplished either by physically protecting the cabling and components that leave a PSP (such as by conduit or secured cable trays) or through data encryption, circuit monitoring, or equally effective logical protections. It is intended that the physical protections reduce the possibility of tampering or allowing direct access to the nonprogrammable devices. Conduit, secured cable trays, and secured communication closets are examples of these types of protections. These physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling and non-programmable components. This could be something as simple as a padlock on a communications closet where the entity would recognize if the padlock had been cut off. Alternatively, this protection may also be accomplished through the use of armored cabling or via the stainless steel or aluminum tube protecting the fiber inside an optical ground wire (OPGW) cable. In using any of these methods, care should be taken to protect the entire length of the cabling including any termination points that may be outside of a defined PSP.

This requirement part only covers those portions of cabling and nonprogrammable communications components that are located outside of the PSP, but inside the ESP. Where these cabling and non-programmable communications components exist inside the PSP, this requirement part no longer applies.

The requirement focuses on physical protection of the communications cabling and components as this is a requirement in a physical security standard and the gap in protection identified by FERC in Order 791 is one of physical protections. However, the requirement part recognizes that there is more than one way to provide protection to communication cabling and nonprogrammable components. In particular, the requirement provides a mechanism for entities to select an alternative to physical security protection that may be chosen in a situation where an entity cannot implement physical security or simply chooses not to implement physical security. The entity is under no obligation to justify or explain why it chose logical protections over physical protections identified in the requirement.

The alternative protective measures identified in the CIP-006-6 R1, Part 1.10 (encryption and circuit monitoring) were identified as acceptable alternatives in NERC petition of the PacifiCorp Interpretation of CIP-006-2 which was approved by FERC (RD10-13-000). If an entity chooses to implement an “an equally effective logical protection” in lieu of one of the protection mechanisms identified in the standard, the entity would be expected to document how the protection is equally effective. NERC explained in its petition of the PacifiCorp Interpretation of CIP-006-2 that the measures are relevant to access or physical tampering. Therefore, the entity may choose to discuss how its protection may provide detection of tampering. The entity may also choose to explain how its protection is equivalent to the other logical options identified in the standard in terms of the CIA triad (confidentiality, integrity, and availability). The entity may find value in reviewing their plans prior to implementation with the regional entity, but there is no obligation to do so.

The intent of the requirement is not to require physical protection of third party components, consistent with FERC Order 791-A. The requirement allows flexibility in that the entity has control of how to design its ESP and also has the ability to extend its ESP outside its PSP via the logical mechanisms specified in CIP-006-6 Requirement 1, Part 1.10 such as encryption (which is an option specifically identified in FERC Order 791-A). These mechanisms should provide sufficient protections to an entity’s BES Cyber Systems while not requiring controls to be implemented on third-party components when entities rely on leased third-party communications.

In addition to the cabling, the components in scope of this requirement part are those components outside of a PSP that could otherwise be considered a BES Cyber Asset or Protected Cyber Asset except that they do not meet the definition of Cyber Asset because they are nonprogrammable. Examples of these nonprogrammable components include, but are not limited to, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the PSP to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the PSP. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. Entities may choose for certain Physical Access Control Systems (PACS) to reside in a PSP (PSP) controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement R1, Parts 1.1, 1.6 and 1.7 beyond what is already required for the PSP.

Regarding Requirement R1, Part 1.10, when cabling and other nonprogrammable components of a Control Center’s communication network cannot be secured in a PSP, steps must be taken to ensure the integrity of the BES Cyber Systems. Exposed communication pathways outside of a PSP necessitate that physical or logical protections be installed to reduce the likelihood that man-in-the-middle attacks could compromise the integrity of their connected BES Cyber Assets or PCAs that are required to reside within PSPs. While it is anticipated that priority consideration will be given to physically securing the cabling and nonprogrammable communications components, the SDT understands that configurations arise when physical access restrictions are not ideal and Responsible Entities are able to reasonably defend their physically exposed communications components through specific additional logical protections.

Rationale for Requirement R2:

To control when personnel without authorized unescorted physical access can be in any PSPs protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Rationale for Requirement R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — System Security Management

Technical Rationale and Justification for Reliability Standard CIP-007-7

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-007-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-007-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-007-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The V5TAG, which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale.pdf" for reference when reading the technical rationale that follows.

General Considerations

Requirement R1

General Considerations for Requirement R1

Shared Cyber Infrastructure (SCI) is mutually exclusive from BES Cyber System (BCS) by definition. To clarify treatment of virtualization concepts in CIP-007-7, the SDT added “SCI supporting an Applicable System in this Part”. This approach keeps the SCI applicability parallel to each existing variant of Applicable Systems in the same Requirement Part (i.e., Medium impact BCS vs. Medium impact BCS with External Routable Connectivity (ERC) vs. Medium impact BCS at Control Centers etc.)

Change Rationale Requirement R1:

The SDT has changed the name of the R1 table to “System Hardening” to clearly reflect the security objective of the entries in the table, which is to reduce a systems’ attack surface. The parts of this requirement do this by:

- limiting network access to only needed routable protocol network accessibility (i.e., logical ports or services),
- limiting access to physical I/O ports (i.e., USB, network, console ports) to only what is necessary, and
- limiting the shared hardware (CPU and memory resources) attack surface between certain groups of VCAs on SCI.

As R1 is broader than only ports and services, the table name was changed to reflect this. The SDT notes that this is merely a label on the Requirement Parts table, linking it to the main Requirement 1 language above it, and does not change or imply any other Requirements or Requirement Parts.

The SDT chose to include “SCI supporting an Applicable System in this Part” language in the Applicable Systems column of the requirement to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the Virtual Cyber Assets (VCA) used in applicable BCS, EACMS, PACS or PCA.

Change Rationale Requirement R1 Part 1.1: Requirement R1 Part 1.1 requires “disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability”. The SDT updated the Requirement Part language to state a security objective concerning “*routable protocol network accessibility*” as opposed to “ports and services”. As this is a new phrase, the intent of this phrase with some examples and rationale for this change is as follows.

> ***Routable protocol network accessibility*** - The objective of this phrase in the Requirement Part is to reduce the attack surface on an applicable system by preventing any unnecessary accessibility to the system over a network using routable protocols. “Accessibility” as used in R1.1 is at the routable protocol network level and does not include physical access, logon to the physical console, code on TCA/RM, etc. Port numbers (TCP/UDP) are at times the best way to track this accessibility, at other times documenting enabled services is better. For example, reducing network accessibility in the physical underlay of SCI between hypervisors or on fabric-based networks may be best performed at a *services* level; turning off or disabling virtualization services that are not needed, rather than documenting the often proprietary and dynamic port numbers which may be of little value. However, in the overlay where an entity may be hosting a database server VCA, it may be easier to show that network accessibility on that VCA is limited to SQL server and remote admin enabled port numbers. In Zero Trust Architectures (ZTA), it may be neither ports or services, but instead a “user to tagged workload” level access control policy where accessibility is described and protected at a more granular, yet higher level than a port #, enforced at a Policy Enforcement Point (PEP) on the applicable system. The SDT has moved to this objective language to avoid prescribing only one way to perform and document network accessibility in all these various scenarios and implementations. In addition, it is limited to routable protocol network accessibility such that non routable network communications (e.g., SAN over Fiber Channel) do not fall within scope of the Requirement Part. The objective is to know the ways a system

can be accessed from the network via routable protocols and have no unnecessary attack surface from that perspective.

In this Requirement Part, the SDT used the verbs “Disable or prevent”. In some cases, the entity may be able to disable a service or remove/uninstall software that is providing unneeded network accessibility to the applicable system. In other cases, the entity may not be able to disable a service, but can prevent access to it in another layer, such as the underlying OS with a host-based firewall, a PEP, or other means of filtering traffic. In instances where the entity can do neither (e.g., a firmware-based ‘black box’ device with limited configuration capabilities), the SDT chose to add ‘per system capability’ to make the requirement conditional on the ability of the applicable system to meet it, if the entity can show that it is incapable.

The SDT also added the clarifier “on each Applicable System” to indicate that the intent of this requirement is for an entity to perform the configuration actions ***on*** each Applicable System, hardening the system from its routable protocol network peers rather than having a single method such as an EAP network firewall rule that would disable such accessibility for a group of Applicable Systems on a network. In other words, merely filtering a port/service on a firewall at an ESP network boundary (CIP-005 R1 controls) does not meet the intent of CIP-007 R1.

Change Rationale Requirement R1 Part 1.3:

Requirement R1 Part 1.3 is a new requirement intended to apply security controls in Shared Cyber Infrastructure scenarios to mitigate the risk of hardware-based vulnerabilities between groups of Applicable Systems of differing impact categorizations. This requirement addresses these vulnerabilities at the CPU and memory level (e.g., Downfall, Inception, Spectre, Meltdown, Rowhammer) that could allow for compromise across processes simultaneously executing on the same shared hardware. Virtualization technology typically has “affinity” controls that can be used to tag VCAs by their impact category and then configure affinity rules such that hypervisors do not instantiate or move VCAs of differing trust levels to the same CPU or memory resources at the same time. Note the requirement excludes shared storage resources, although included in the definition of SCI. The SDT intent is it is allowable to have logical disks attached to systems of differing impact categorization stored in the same SAN for example, and since these storage solutions have internal CPU and memory, which is not the intended object of this requirement.

Note that the SCI definition covers *only* those portions of entity’s virtualization infrastructure that support systems of differing impact levels. As VCAs that share the same CPU or memory with any part of the highest rated BCS are “Associated PCAs”, this requirement is only needed to cover instances where different impact categorizations are supported and the entity wishes to keep other VCAs from becoming “associated PCAs’, thus maintaining the separation by impact category. This may occur when part of the same SCI supports different BCS and the entity does not wish to high watermark all the BCS together, but instead employ affinity rules to prevent VCAs that are high or medium impact from being instantiated or moved to CPU and memory resources where other VCAs are executing.

For example, this requirement would apply where the same SCI supports both a high impact BCS on one part of a virtualization cluster and a low impact BCS on a different part of the virtualization cluster. The proper use of host affinity controls would not require the low impact BCS to be considered an “associated PCA” of the high as long as:

1. the low impact BCS is not in the ESP of the high impact BCS, and
2. controls are in place to prevent the SCI from executing these BCS on the same CPU and memory resources.

As an example, if an entity has a substation intelligent electronic device (IED) management system that is used as an EACMS for medium and low impact BCS in a single VCA, it is an associated EACMS of the medium impact BCS and protected as such. It can therefore execute on hypervisors with other medium or high impact BCS. If it is implemented as two separate VCAs, one for medium impact IEDs and another for low impact IEDs, then the low impact one cannot execute on the same hypervisor as the medium impact one, unless it is categorized as an “associated PCA” of the medium BCS as well. If the entity wishes to have it remain as low impact those two VCAs sharing the same CPU or memory resources would not meet this requirement. In situations where high or medium impact VCAs are allowed to execute on the same CPU or memory resources with VCA's of other impact levels and those other VCA's are inadvertent PCAs, this requirement is a single place for that violation rather than every requirement that has PCA in the scope.

Requirement R2

Change Rationale Requirement R2:

The SDT chose to include the "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA(s) used in applicable BCS, EACMS, PACS or PCA.

The SDT made conforming changes where necessary with Requirement R2 to remove reliance on the Cyber Asset term, choosing to reference the Applicable Systems instead.

Additionally, the SDT chose to insert the word "cyber" as a clarifier to security patches for consistency with the term used in R2.1.

Backward Compatibility

CIP-007-7 Requirement R2 retains backward compatibility for entities that do not utilize SCI.

The SDT intends that entities take full advantage of their virtualization infrastructure in order to ease the overhead associated with patch management. While many of the entity's existing processes will remain the same, (such as those associated with tracking the source of cyber security patches, evaluation of the applicability of available patches and mitigation plans for those applicable patches that cannot be installed) new or modified processes around the installation of patches can be used (for example, parent images, remediation VLANs, etc.).

Parent Images

One of the interesting nuances of virtualization is the concept of parent/child relationships.

Some VCAs utilize a "parent image" type methodology where a specific VCA (operating system and software) is merely a child instance of a parent image. In such cases, the application of cyber security patches to the parent image applies those changes to any children instantiated from that image. As there may be many dynamic child instances, the administrative overhead associated with patching of those child instances can be greatly reduced. The intent is that entities would track and document the R2 cyber security patching requirements at the parent image level rather than attempting to track and document patching for each individual VCA instantiated from the parent image.

Dormant Instances

There are times when a VCA may not be in use and, as a virtual instance, may be shut down to free its resources since it can be easily instantiated when needed. Thus, VCAs are unlike physical Cyber Assets that are up and running continuously and can receive applicable patches, software updates, configuration updates, etc.

Leveraging the built-in virtualization features allows idle resources to be reassigned to tasks at hand without incurring additional overhead of tracking which dormant virtual instances require patching. Dormant virtual instances are just files with the saved state of the VCA. Dormant instances are not VCAs themselves nor Applicable Systems until they become active instances again.

Where a dormant virtual instance is also the child instance of a parent image, the application of security patches to the parent image will also make the same changes automatically when needed to any out of date dormant child virtual instances when they are restarted.

In most cases, a dormant virtual child instance is made active again on a remediation type network where any missing security patches (compared to the parent image) are automatically applied before it is placed back into active service.

Saved Images

Similar to dormant child images, saved child images or snapshots may be also used as functional backups for CIP-009 purposes in order to provide fast restoration and better availability. If an active VCA becomes corrupted, a saved image can be made active where the application of any missing security patches (compared to the parent image) can be automatically applied, through remediation, before being placed back into active service. However, the SDT's intent is that VCA images that are used for backup purposes would not be subject to patching, as the backup may be needed to recover from a failed patch or if later discovered that a patch has negatively affected functionality.

Requirement R3

Change Rationale Requirement R3:

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA.

Requirement R4

Change Rationale Requirement R4:

The SDT chose to include "SCI supporting an Applicable System in this Part" language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCA.

Change Rationale Requirement R4 Part 4.1:

The SDT determined the entire structure of the "at the BCS level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability)" language could be simplified to "per system capability" since the Applicable Systems column clarifies what systems are included.

Additionally, the SDT chose to insert the word "security" as a clarifier to which events are to be logged.

Change Rationale Requirement R4 Part 4.2:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the "Cyber Asset" term, as well as the ambiguity that would have existed if the term "BES Cyber System" were left in place while the Applicability Column included SCI.

Change Rationale Requirement R4 Part 4.3:

The SDT clarified the retaining of applicable "security" event logs, as that is what is identified in Part 4.1.

The SDT also chose to remove the reliance on a TFE from Part 4.3 in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

Requirement R5

Change Rationale Requirement R5:

The SDT chose to include “SCI supporting an Applicable System in this Part” language in the Applicable Systems column of the requirement in order to ensure that controls which are applicable to the hardware portion of a physical Cyber Asset would remain applicable to the hardware supporting the VCA used in applicable BCS, EACMS, PACS or PCAs.

Change Rationale Requirement R5 Parts 5.1, and 5.6 – 5.7:

The SDT chose to remove the reliance on TFE in favor of the updated term “per system capability”. The SDT contends that the term still requires an entity to document the limit to the system’s capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

Change Rationale Requirement R5 Part 5.4:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the “Cyber Asset” term, replacing it with a per “system” capability.

Change Rationale Requirement R5 Part 5.5:

The SDT applied conforming changes to the Requirement Part language to remove the reliance on the “Cyber Asset” term, replacing it with a reference to the Applicable Systems.

Former Background Section from Reliability Standard CIP-007-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-007-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-007-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

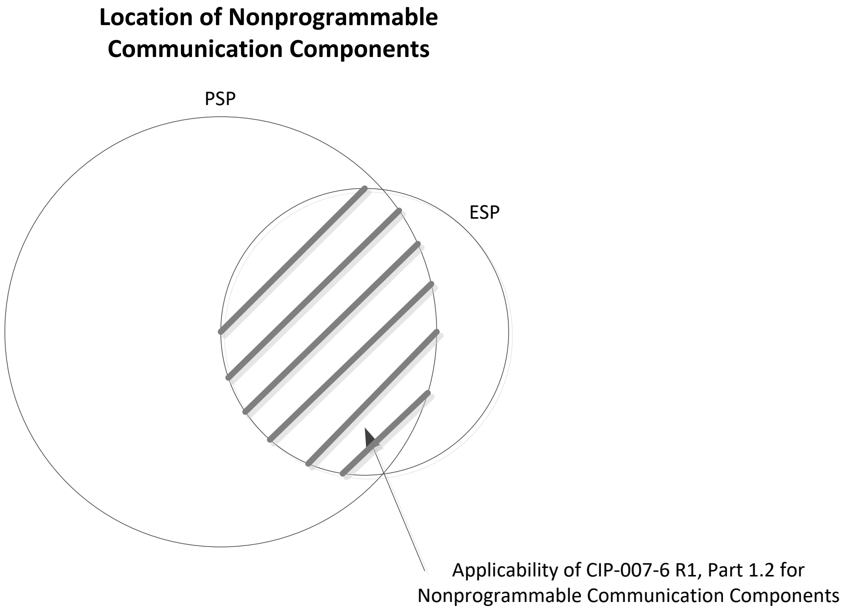
The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

The network ports included in the scope of this requirement part are not limited to those on the BES Cyber System itself. The scope of physical network ports includes those ports that may exist on nonprogrammable devices such as unmanaged switches, hubs, or patch panels.

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

The Applicable Systems column was updated on CIP-007-6 Requirement 1, Part 1.2 to include "Nonprogrammable communication components located inside both a PSP and an ESP." This should be interpreted to apply to only those nonprogrammable communication components that are inside both an ESP and a PSP in combination, not those components that are in only one perimeter as can be illustrated in the following diagram:



Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Standalone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. A patch source is not required for Cyber Assets that have no updateable software or firmware (there is no user accessible way to update the internal software or firmware executing on the Cyber Asset), or those Cyber Assets that have no existing source of patches such as vendors that no longer exist. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 2. Determination that a security related patch, hotfix, and/or update poses too great a risk to install on a system or is not applicable due to the system configuration should not require a TFE.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

Entities should also have awareness of malware protection requirements for Transient Cyber Assets and Removable Media (“transient devices”) in CIP-010-2. The protections required here in CIP-007-6, Requirement R3 complement, but do not meet, the additional obligations for transient devices.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System’s ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a ‘false positive’ could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of Removable Media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc.). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement’s rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or "special" characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

In response to FERC Order No. 791, specifically FERC's reference to NIST 800-53 rev. 3 security control PE-4 in paragraph 149, Part 1.2 has been expanded to include PCAs and nonprogrammable communications components. This increase in applicability expands the scope of devices that receive the protection afforded by the defense-in-depth control included in Requirement R1, Part 1.2.

The applicability is limited to those nonprogrammable communications components located both inside a PSP and an ESP in order to allow for a scenario in which a Responsible Entity may implement an extended ESP (with corresponding logical protections identified in CIP-006, Requirement R1, Part 1.10). In this scenario, nonprogrammable components of the communication network may exist out of the Responsible Entity's control (i.e. as part of the telecommunication carrier's network).

Rationale for Requirement R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

Rationale for Requirement R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Rationale for Requirement R4:

Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Rationale for Requirement R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security – Incident Reporting and Response Planning

Technical Rationale and Justification for Reliability Standard CIP-008-7

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-008-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-008-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 – Requirement R4

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-008-6 to align incident reporting and response planning requirements with the virtualization changes and protections for Shared Cyber Infrastructure (SCI) by adding "SCI supporting an Applicable System in this Part" to each of the Parts in Applicable Systems for Requirement R1 – Requirement R4.

Requirement R4

Rationale

The Project 2016-02 SDT made updates to reflect the change from the National Cybersecurity and Communications integration Center (NCCIC) to its successor organization Cybersecurity & Infrastructure Security Agency (CISA), and deleted the historical footnote in favor of deference to the Requirement language, which already states "or their successors".

Former Background Section from Reliability Standard CIP-008-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-008 exists as part of a suite of CIP Standards related to cyber security. CIP-002 requires the initial identification and categorization of BES Cyber Systems. CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, and CIP-011 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a particular subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST")

Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.

Medium Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.

Technical Rationale for Reliability Standard CIP-008-6

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-008-6. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on the Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-008-6 is not a Reliability Standard and should not be considered mandatory and enforceable.

On July 19, 2018, the Federal Energy Regulatory Commission (FERC or Commission) issued Order No. 848. In this Order FERC directed the North American Electric Reliability Corporation (NERC) to "develop and submit modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access and Control or Monitoring System (EACMS)." (Order 848, Paragraph 1)

In response to the directive in Order No. 848, the Project 2018-02 SDT drafted Reliability Standard CIP-008-6 to require Responsible Entities to implement methods augmenting the mandatory reporting of Cyber Security Incidents to include: "(1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report included specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT)." (Order 848, Paragraph 3)[1]

New and Modified Terms Used in NERC Reliability Standards

CIP-006-6 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms:

Cyber Security Incident

A malicious act or suspicious event that:

- *For a high or medium impact BES Cyber System, compromises, or attempts to compromise the, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or*
- *Disrupts, or attempts to disrupt, the operation of a BES Cyber System.*

In response to FERC Order 848, Paragraph 1, the SDT modified the Cyber Security Incident definition to include Electronic Access Control or Monitoring Systems (EACMS) associated with high or medium impact BES Cyber Systems, in response to the Order.

The addition of high and medium impact BES Cyber Systems considers the potential unintended consequences with the use of the existing definition in CIP-003-7. It also provides clarity that only low impact BES Cyber Systems are

---

[1] The National Cybersecurity and Communications Integration Center (NCCIC) is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In 2017, NCCIC realigned its organizational structure and integrated like functions previously performed independently by the ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT).

included within the definition. ESP or EACMs that may be defined by an entity for low impact BES Cyber Systems are not part of the definition.

An attempt to disrupt the operation of a BES Cyber System is meant to include, among other things, a compromise of a single BES Cyber Asset within a BES Cyber System. For example, malware discovered on a BES Cyber Asset is an attempt to disrupt the operation of that BES Cyber System.

Reportable Cyber Security Incident
A Cyber Security Incident that compromised or disrupted:

- *A BES Cyber System that performs one or more reliability tasks of a functional entity;*
- *An Electronic Security Perimeter of a high or medium impact BES Cyber System; or*
- *An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber Systems.*

The Reportable Cyber Security Incident definition was modified to comply with FERC Order 848. In response to Paragraph 54 of the Order, the SDT modified the definition to include incidents that compromised or disrupted an ESP or an EACMS. The team also added the qualifying clause for "A BES Cyber System that performs one or more reliability tasks of a functional entity" to clarify what was compromised or disrupted, thus not extending the scope to Protected Cyber Assets (PCAs). In response to comments, the SDT left the entire definition of BES Cyber system in Reportable Cyber Security Incident to provide clarity.

It is also important to understand the relationship between the two definitions, the requirement language, and how they work in concert to classify events and conditions at varied levels of significance as the Registered Entity executes its process and applies its defined criteria to determine if reporting is required.

Electronic Access Control or Monitoring Systems (EACMS)
The drafting team spent significant time discussing this topic among its members, through industry outreach, and with FERC staff. The team believes by not specifically referencing the five functions in Order 848, we have reduced complexity and made compliance with the Standard achievable. The drafting team asserts that the five functions are equivalent to the current definition of EACMS in the NERC Glossary of Terms. If entities have questions about application of the EACMS definition, the drafting team advises entities to discuss those questions directly with NERC.

Requirements R1, R2, and R3

General Considerations for Requirement R1, Requirement R2, and Requirement R3

FERC Order 848, Paragraph 1, directs modifications to Reliability Standards to require reporting of incidents that compromise, or attempt to compromise a responsible entity's ESP or associated EACMS. The intent of the SDT was to minimize the changes within CIP-008 and address the required modifications. To do this, the SDT added "and their associated EACMS" to the "Applicable Systems" column for Requirements R1, R2, and R3.

To add clarity to "attempts to compromise," the drafting team created Part 1.2.1 to require entities to establish and document their process to include criteria to evaluate and define attempts to compromise. This requirement maps to Requirement 4 Part 4.2, which requires entities to use that entity-defined process for determining which incidents entities must report.

The use of the language describing Cyber Security Incident(s) as being "an attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the 'Applicable Systems'" column for the Part is meant to clarify which Cyber Assets are in scope for attempts to compromise reporting by entities. This language is used throughout the standard.

Moving Parts of Requirement R1 to Requirement R4

To minimize the changes to Requirement R1, the SDT created Requirement R4 and consolidated all the CIP-008-6 reporting requirements. The SDT deleted Requirement R1 Part 1.2 reporting requirements from CIP-008-5, and moved them to Requirement R4 for this purpose.

Inclusion of "Successor Organizations" throughout the Requirement Parts

The SDT recognizes that organizations are constantly evolving to meet emerging needs, and may re-organize or change their names over time. The ICS-CERT has completed its name change to the National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems. The E-ISAC previously re-branded its name and may again in the future. By following Requirement R4 references to E-ISAC and NCCIC with "or their successors" the SDT is ensuring that Requirement R4 can be implemented even if the names of E-ISAC and NCCIC change or a different agency takes over their current roles.

Requirement R4

General Considerations for Requirement R4

Requirement R4 is a new requirement focused on mandatory reporting of Reportable Cyber Security Incidents and includes attempts to compromise systems in the "Applicable Systems" column. Previously, CIP-008-5 defined reporting requirements for Reportable Cyber Security Requirements (Requirement R1 Part 1.2) only.

Required Reportable Incident Attributes

Requirement R4.1 specifies that initial notifications and updates must include three attributes: 1) functional impact, 2) attack vector used, and 3) level of intrusion achieved or attempted. These attributes are taken directly from the Order. (FERC Order No. 848, paragraph 89).

The SDT understands that some or all of these attributes may be unknown at time of initial notification. To account for this scenario the SDT included "to the extent known" in the requirement language. There is an expectation that update reporting will be done as new information is determined or unknown attributes become known by the entity. There could be cases, due to operational need, that all the attributes may never be known, if this case presents itself that information should be reported.

Methods for Submitting Notifications

Requirement R4 Part 4.2 allows responsible entities to submit notification using any method supported by E-ISAC and NCCIC. The SDT did not prescribe a particular reporting method or format to allow responsible entities' personnel to focus on incident response itself and not the method or format of reporting. It is important to note the report must contain the three attributes required in Requirement R4 Part 4.1 as they are known, regardless of reporting method or format.

Notification Timing

Requirement R4 Part 4.2 specifies two timelines for initial notification submission; one hour for Reportable Cyber Security Incidents; and end of next calendar day for attempts to compromise systems in the "Applicable Systems" column. Paragraph 3 of FERC Order No 848 directly states that reporting deadlines must be established. Paragraph 89 further states that "timelines that are commensurate with the adverse impact to the BES that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES."

- *Reportable Cyber Security Incidents* – The SDT wrote Requirement R4 Part R4.2 to use a one hour deadline for reporting of these events because incidents in this category include successful compromise of ESP(s), EACMS, or BES Cyber System(s). One hour is referenced directly in FERC Order No 848 paragraph 89 and is also the current reporting requirement in CIP-008-5.
- *Cyber Security Incident that was an attempt to compromise one or more systems identified in the "Applicable Systems" column* - Due to the lower severity of these unsuccessful attempts at compromising ESP(s), EACMS, or BES Cyber System(s), the SDT proposed a longer reporting timeframe. The intent behind

> the decision to add "By the end of the next calendar day" (11:59 pm local time) was to give responsible entities additional time to gather facts prior to notifications for the less severe attempts to compromise Applicable Systems. It is important to note that compliance timing begins with the entity's determination that attempt to compromise meets the process they defined in Requirement R1 Part 1.2.1.

The SDT understands initial notification may not have all the details when first submitted. It is expected, however, that information that has been determined is reported within the notification deadlines. Additionally, it is important to note the wording in Requirement R4 Part 4.2. The "compliance clock" for the report timing begins when the Responsible Entity executes its process from Requirement R1 Part 1.2.1 and a determination has been made that the type of incident which has occurred qualifies as reportable.

Technical rationale taken from the Guidelines and Technical Basis (GTB) CIP-008-5 Requirement 1 provides additional justification for the SDT to maintain the one hour timeframe for Reportable Cyber Security Incidents.

> *"The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."*

In 2007, the Electricity Information Sharing and Analysis Center (E-ISAC) was known as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Its voluntary procedures required the reporting of a cyber-incident within one hour of an incident. CIP-008-1 required entities to report to the ES-ISAC.

In FERC Order No. 706[2] (July 18, 2008), the Commission concluded that the one-hour reporting limit was reasonable [P 663]. The Commission further stated that it was leaving the details to NERC, but it wanted the reporting timeframe to run from the "**discovery**" of the incident by the entity, and not the actual **"occurrence"** of the incident [P 664].

CIP-008-2 and CIP-008-3 were silent regarding the required timeframe for reporting, but it was specifically addressed in CIP-008-5. In the October 26, 2012, redlined version of CIP-008-5, the proposed language for initial notification originally specified "one hour from **identification**" of an incident. This aligned with the Commission's decision in Order No. 706, for the clock to start with the discovery of an incident. However, the Standard Drafting Team changed "one hour from identification" to "one hour from the **determination** of a Reportable Cyber Security Incident". This language was subsequently approved and incorporated into CIP-008-5.

These changes, from "occurrence" to "discovery" to "determination," provide the additional time needed for the entity to apply its specifically created process(es) for determining whether a Cyber Security Incident rises to the level of required reporting. This determination timeframe may include a preliminary investigation of the incident which will provide useful information to other entities to help defend against similar attacks.

Notification Updates

Requirement R4 Part 4.3 requires that Responsible Entities submit updates for the required attributes upon determination of new or changed attribute information, if any. The SDT added this language to provide entities sufficient time to determine attribute information, which may be unknown at the time of initial notification, and which may change as more information is gathered. The intent of Requirement R4 Part 4.3 is to provide a method for Responsible Entities to report new information over time as their investigations progress. NOTE: The SDT does not

---

[2] 2008, Federal Energy Regulatory Commission, Mandatory Reliability Standards for Critical Infrastructure Protection, Order No. 706.

intend updates specified in Requirement R4. Part 4.3 to expose responsible entities to potential violations if, for example, initial and updated notification on the same attribute have different information. This is expected since knowledge of attributes may change as investigations proceed. Rather, the intent of Requirement R4 Part 4.3 is to have a mechanism to report incident information to E-ISAC and NCCIC (and thereby industry) upon determination of each required attribute.

The intent is that the entity report what is known and document the reason not all attributes could become known and ultimately be reported in conditions where, e.g. a Cyber Asset was restored completely, removing all forensic evidence in order to restore operations, which caused the entity to conclude its investigation without having a complete knowledge of the three required attributes.

The SDT asserts that nothing included in the new reporting Requirement R4, precludes the entity from continuing to provide any voluntary sharing they may already be conducting today.

Technical Rationale for Reliability Standard CIP-008-5

This section contains the Guidelines and Technical basis as a “cut and paste” from CIP-008-5 standard to preserve any historical references.

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5’s categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for Reportable Cyber Security Incidents.

Entities may use an actual response to a Reportable Cyber Security Incident as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise.

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for Reportable Cyber Security Incidents. There are several examples of specific types of evidence listed in the measure.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response activities. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

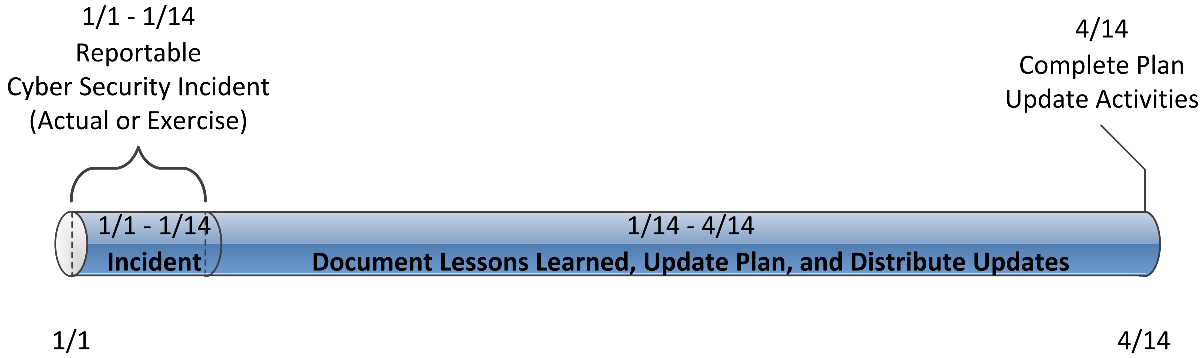
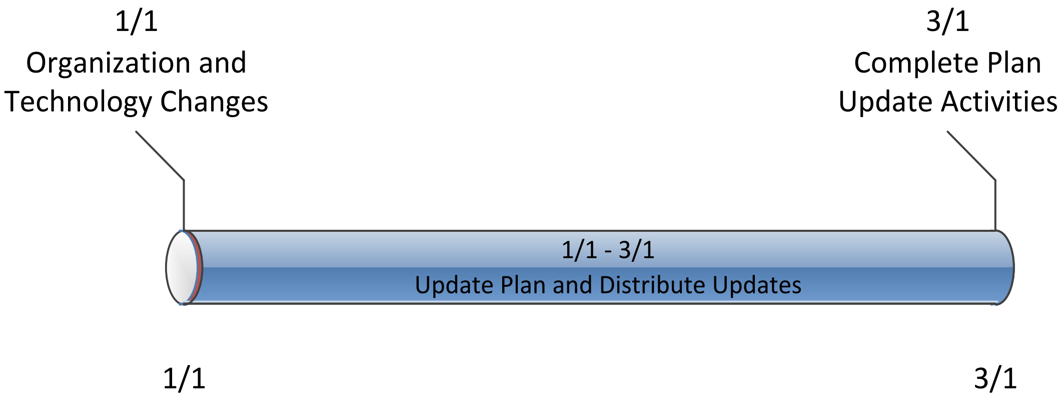


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in **Error! Reference source not found.**, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals.

Figure 2: Timeline for Plan Changes in 3.2



Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)
"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)
Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)
Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)
Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)
Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)
Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)
Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Recovery Plans for BES Cyber Systems

Technical Rationale and Justification for Reliability Standard CIP-009-7

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-009-7

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-009-7. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-009-7 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition Advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received addressing the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1 – Requirement R3

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-009-7 to align recovery planning requirements with the virtualization changes and Shared Cyber Infrastructure (SCI).

The use of the term BES Cyber System has been replaced with “Applicable System” within the requirement language of Requirement R1 Part 1.3 and Requirement R2 Part 2.2 to align the requirement with the applicability for each Requirement Part.

Requirement R1 Part 1.5 has added ‘SCI supporting an Applicable System in this Part’ to the applicability. This requires that SCI be included in the process to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Having any SCI included in the forensics for a compromised applicable VCA, or the SCI itself, is the reason for the inclusion.

SCI is not specifically included in any other Requirement Parts of CIP-009, because CIP-009 focuses on the ability to recover the BCS functionality, which may or may not require recovery of SCI. The SDT has therefore not included SCI as a direct object of the other recovery plan Requirements and Parts. However, if recovery of the Applicable System’s functionality is dependent on recovery of any SCI, then the recovery plan(s) should include such dependencies.

Former Background Section from Reliability Standard CIP-009-6

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-009 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements.

An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

Technical Rationale for Reliability Standard CIP-009-6

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-009-6 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Reliability Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, “A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Tabletop exercises (TTX)] can be used to assess plans, policies, and procedures.”

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, “[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and ‘boots on the ground’ response (e.g., firefighters decontaminating mock victims).”

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

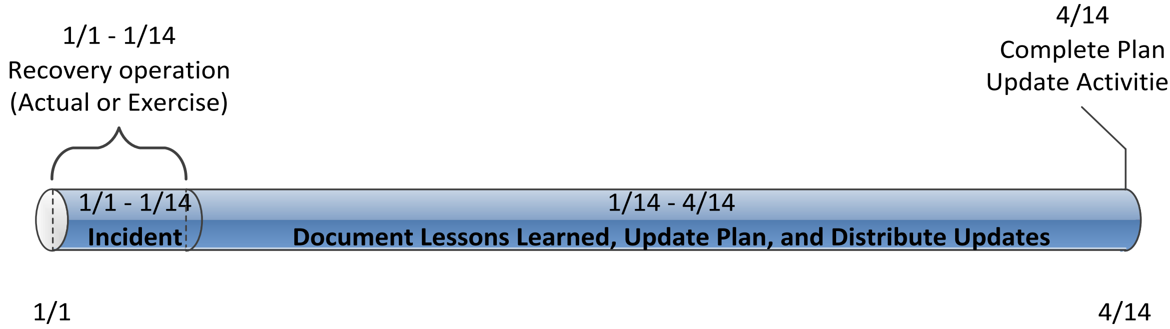


Figure 1: CIP-009-6 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

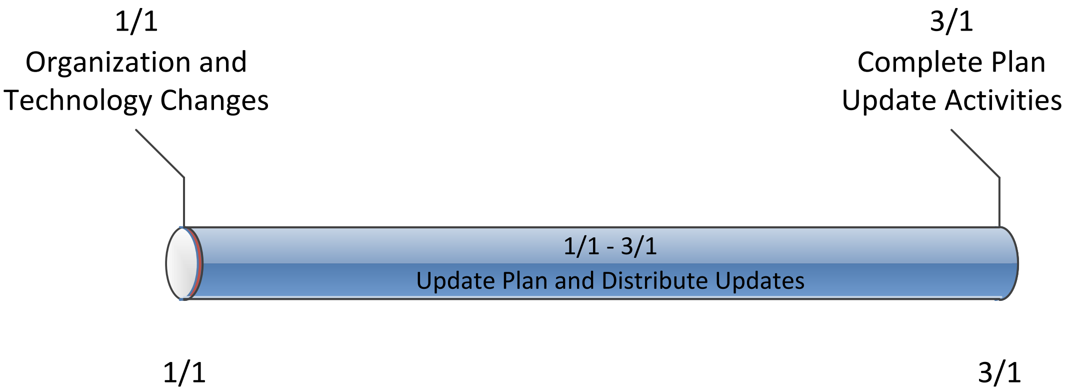


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Rationale for Requirement R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Rationale for Requirement R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Change Management and Vulnerability Assessments

Technical Rationale and Justification for Reliability Standard CIP-010-5

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-010-5

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-5. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-010-5 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server, and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference.

Virtualization Concepts Driving CIP-010 Changes

The proposed changes in CIP-010-5 from the Project 2016-02 SDT concern the use of several facets of virtualization technologies. Virtualization allows for such technologies as new controls for Shared Cyber Infrastructure (SCI), remediation VLAN, containers, parent/child images, and dormant virtual machines (VMs). Enabling and clarifying the use of these technologies is the basis of the proposed changes in CIP-010-5. A general introduction to each of these technologies follows.

Shared Cyber Infrastructure (SCI)

Where entries elect to utilize "Shared Cyber Infrastructure", virtualization abstracts the software layers (the OS and applications) from the underlying hardware to allow the hardware infrastructure to be shared among several Virtual Cyber Assets (VCAs) that may be of differing impact levels. Hypervisors must include security controls to keep these workloads logically isolated from one another and those requirements are within other CIP standards such as CIP-005 and CIP-007. However, with any type of shared infrastructure, the need for change management requirements is elevated for those security controls that allow for the 'shared' in SCI. Such controls are added to the change management requirements in CIP-010-5. As discussed elsewhere, entities may choose to high watermark all VCAs executing in their virtualized infrastructure, known as the "all-in" scenario, and not be concerned with SCI specific requirements. They simply consider the underlay part of the highest impact BCS executing on it and comply with the appropriate security controls and requirements for it.

Remediation VLAN

Remediation VLAN is a term used to describe a logical network segment in which a Cyber Asset or VCA can be isolated from having routable connectivity to any BES Cyber Systems (typically only having visibility of remediation services such as patching and antimalware updates, etc.) while it is examined to ensure the integrity and validity of the configuration and software installed on it. After this examination and subsequent remediation of deficiencies is completed, it is then joined to its production network.

This examination is policy driven, meaning that the administrator is able to configure what the minimum requirements are for a successful examination. Examples of this might be minimum operating system patch levels or recent anti-virus definitions.

If during the examination of the asset, it is found to not comply with the requirements defined in the policy, an administrator may intervene to manually remediate the deficiencies, or the system which was used to examine the asset may communicate the deficiencies to the asset with instructions on how to remediate itself in an automated fashion. After the remediation actions are taken, the asset can request to be re-examined and if the requirements dictated by the policy are now met, it will be joined to its production network.

Containers (Application Containers)

Containers are a form of virtualization at an individual application level, bundling the application code and its runtime environment into a self-contained, sandboxed environment. The application can then be instantiated dynamically on one or multiple dynamic hosts. The benefit is it makes the application or logic as portable as possible and able to be instantiated as-is without modification on a developer's workstation, a test environment, or a production data center without the notion of installing the application or the various runtime dependencies into a particular OS instance. This notion of applications no longer being installed into an OS has significant implications for previous versions of CIP-010 R1 which were based almost solely on a 'baseline configuration' of installed software. The images from which application containers are instantiated that meet the conditions of R1.1 should not be outside the scope of change authorization because they are not "installed" in a particular instance of an OS. To limit R1 to only "installed" software may leave out the way applications are beginning to be delivered in systems of today.

Parent/Child Images

When a VCA is 'powered on' or begins execution, it instantiates ("boots") from a disk image file. Since the boot 'disk' is a file and not physical disk, many individual VCAs can use the same "parent" image as the basis for their own "child" image. Among other things, this allows for patching of an OS to occur to a parent image and the child images then pick up that patched image upon their next instantiation. A common use of parent/child images is Virtual Desktop Infrastructures (VDI) that deliver a temporary desktop environment to each remote user for the duration of their session that are VCAs instantiated from a parent image.

Dormant VMs

A VCA that is not currently executing or instantiated (i.e., not 'booted up') is a dormant VM. It exists not as a traditional VCA, but simply as a file. VCA's can be created for specialized purposes such as to run troubleshooting tools and are only instantiated when needed and may be dormant for long periods of time. They are not instantiated and on the network where they are managed and patched on a regular basis. However, these can go hand-in-hand with remediation VLANs which would bring them up to date as soon as they do begin to instantiate.

General Considerations

SCI is mutually exclusive from Cyber Assets (CA) by definition. To enable CIP-010-5 for virtualization, the SDT evaluated the existing Applicable Systems and added "SCI that supports an Applicable System in this Part". This approach keeps the SCI applicability parallel to each existing variant of Medium Impact BCS (i.e. Medium Impact BCS vs. Medium Impact BCS with External Routable Connectivity (ERC) vs. Medium Impact BCS at Control Centers etc.).

Requirement R1

General Considerations for Requirement R1

In prior versions, CIP-010 Requirement R1 has required developing a baseline configuration that consisted of five (5) items (OS or firmware, installed and custom software, ports, and patches). The baseline configuration was then used in the remainder of Requirement R1 and R2 as the basis of change management including testing. At a high level, the CIP-010-4 Requirement Part 1.1 was to develop a baseline configuration, Requirement R1 Part 1.2 was to authorize and document changes to the items in the baseline configuration, and Requirement R1 Part 1.3 was to update the baseline configuration within a specific timeframe after a change. This tended to focus the requirement on maintaining documentation of past changes. However, in CIP-010-4 the core security objective of R1 was in Part 1.2 to authorize and document changes and the baseline configuration was used primarily to set the scope of those changes. Maintaining the baseline configuration information within 30 days after making changes is not a security objective, and as we implement more dynamic systems and more automation of change with virtualization, it becomes more problematic.

In CIP-010-5, the SDT considered the more dynamic, policy-based, and automated virtualization technologies discussed in the previous section and determined to focus Requirement R1 on the true security objective of change management and authorizing intended changes for those changes that can affect the security posture. In other words, make R1.2 from version 4 the main focal point in version 5. Maintaining documentation of ever more automated updates to systems after the fact gives way in this version to authorizing changes that will affect the security posture of the system. The SDT is addressing VCA's that may be dormant for long periods of time and dynamically patched at a future instantiation when needed. The SDT considered the focus of R1 is not for entities to track the date/time a VCA may be dynamically instantiated and patched in an automated fashion in a remediation VLAN and then provide evidence that a baseline configuration was updated within 30 days of that dynamic event.

In addition, with the introduction of application containers and orchestration (Kubernetes, Docker Swarm, etc.), application software may no longer be "installed" on a particular OS instance on a particular server. Instead, an orchestration service may instantiate an application container on the best "node" (server with container runtime) at the moment. For example, a dedicated "database server" gives way to a "database service" that can be instantiated in a container on any VCA or CA managed by the orchestrator. Therefore, baseline configurations of statically installed software and open ports loses value as it becomes dynamically managed in these scenarios. The focus of R1 has thus changed from documenting the installed software and its open ports on a Cyber Asset or VCA at some point post-change to authorizing the changes that will occur to it when it does instantiate, which provides more security value.

Entities may of course continue to maintain and use baseline configurations, but in CIP-010-5 it is no longer the singular prescribed way of setting change management scope and documenting changes. Baseline configurations may continue to be used as evidence for CIP-007 R1 for example, documenting the enabled ports on a system. In fact, baseline configurations will probably continue to be a very common method used by entities to help detect unauthorized changes in CIP-010 R2, but the standard does not prescribe it as the singular way to meet these security objectives. Therefore, the phrase "baseline configuration" has been removed from CIP-010-5 though entities may continue using it as their "how". Again, the focus of R1 in CIP-010-4 and CIP-010-5 is authorizing changes that affect the security posture of the applicable systems; the SDT has just brough it forward as the "what" with baseline configurations as one possible, but not prescribed, "how". Entities may also wish to reference NIST SP 800-128 "Guide for Security-Focused Configuration Management of Information Systems" as a guide for additional information.

The SDT also considered at length the scope of changes that should be subject to R1. In CIP-010-4, the scope was set by the prescribed elements in the baseline config, consisting essentially of software, patches, and ports. As mentioned above, the security objective of putting ports in the baseline configuration is not to document and maintain a list of listening ports; that security objective is covered in CIP-007 R1 to reduce the attack surface by disabling unneeded ports. Maintaining documentation of the patches installed on a system (which becomes more problematic over time with vendor-bundled monthly updates that may install/remove patches differently per each system's needs) is not the security objective. Knowing what patches are available and applicable to the systems and installing them and mitigating the risk is the goal as covered in CIP-007 R2. In CIP-010 R1, authorizing the action in order to manage change is the objective.

In addition, the SDT considered the prescribed list of baseline configuration elements was insufficient as the scope of a change management requirement. For example, in an SCI that is configured to isolate VCAs of different impact levels from each other, managing and authorizing change to that configuration is vital. As Zero Trust architectures come to fruition, managing and authorizing changes to those access policies is crucial. These are all very important security configurations that were not enumerated in CIP-010-4's baseline configuration and thus not in scope. The SDT concluded that creating a longer prescriptive list of items was not appropriate, in that such a list would need to be maintained as technology changes. The SDT decided to put objective language in the requirement and use the Measures to show examples of more detailed lists of items.

Rationale for Requirement R1 Part 1.1

The SDT brought the security objective to the forefront in this requirement part by starting it with "Authorize changes…". Next it narrows the scope to those "that affect Applicable Systems" and the SDT made conforming changes to Applicable Systems to add SCI. The SDT considered that many entities scope their own internal change management processes this way; if a change is to or affects something in their NERC CIP program for medium/highs, it goes through change management. However, the requirement needs a bit more precise scoping accomplished with the objective language of "…altered behaviors…" to the underlying technical controls so it doesn't include changes such as a user changing their password or desktop background, or a system log being written to hundreds of times an hour. The requirement needs a lower bound, a floor, without attempting to incorporate a prescriptive list of change types or categories.

The SDT used the objective language "…where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 and CIP-007, as defined by the Responsible Entity." The intent is to bound the scope to those changes that affect the system's CIP security posture. *More precisely, the intent is to set the floor of the scope to changes that alter the behavior of a cyber security control the entity uses to keep the system secure per CIP-005 and CIP-007 requirements.*

The phrasing "alter the behavior of one or more cyber security controls" is intended to help clarify the scope. For example, the intent is that a user changing their password is not in scope; that is a change that may be required on some periodicity by a cyber security control such as a domain password policy but is not a change that alters the behavior *of the control itself*. What would be in scope is a change to that domain password policy.

The "excluding procedural and physical controls" (as well as the "*cyber security* controls" phrase) is intended to exclude from CIP-010 R1's scope changes to controls from CIP-005 and CIP-007 that are not technical controls. An example would be an entity may have signage or port-blockers as a procedural/physical control for meeting CIP-007 R1.2 concerning physical ports. Installing/removing port blockers or changes to the signage is not intended to be subject to CIP-010 R1. A change to the affinity rules for a hypervisor, if the entity uses that in an SCI scenario to meet CIP-007 R1.3, would meet the intent, as well as changes to EAP firewall rules/policy that the entity uses as the control to meet CIP-005 R1. The configuration of anti-malware controls the entity uses, such as update mechanisms or alerting mechanisms that change *how* the control functions in meeting CIP-007 R3 would be included but not the regular signature updates the control uses; those are not changes to the control's configuration that alter the way the control behaves.

Along these lines, rather than including a prescriptive list of change categories or types within the requirement, the SDT did analyze the requirements in CIP-005 and CIP-007 and included examples of cyber security controls that may serve those requirements in the Measures column to help clarify the intent. These are examples and are not a mandatory prescriptive list of the types of changes that would be included and for which evidence of authorization through change records could be provided.

It is important to note the SDT did not include prescriptive timeframes for this requirement. The rationale for this is to account for emergency changes, those that need to occur for reliability of the system when it may not be possible to put in a request and gain authorization beforehand. The SDT intent is for these system reliability related emergency changes to not become a violation of this standard, which it would if it had “prior to” type phrases within it, or required prescriptive definition of what constitutes emergency changes, etc. However, emergency changes will still need to be authorized, after the fact, to meet the requirement.

Rationale for Requirement R1 Part 1.2

Requirement R1 Part 1.2 is where CIP-010-4 Requirement R1 Part 1.5 now lands in CIP-010-5, with minor modifications to Part 1.2.1, and conforming changes to remove the ‘baseline configuration’ terminology to enable for virtualization.

The SDT chose to remove the reliance on a “Technical Feasibility Exception” in favor of permitting “CIP Exceptional Circumstances” in Part 1.2.1. The SDT contends testing in a test environment prior to implementing any change in production, and documenting test results may impede Responsible Entities' efforts to recover from events or conditions that qualify as CIP Exceptional Circumstances, and that term still requires an entity to document when that condition occurs with regards to the requirement language, while not incurring the additional documentation overhead of a Technical Feasibility Exception (TFE).

Additionally, Requirement R1 language negates the need for both the “technically feasible” and “per system capability” because the focus is on testing the implemented CIP-005 and/or CIP-007 cybersecurity controls the responsible entity determines as serving the requirements in CIP-005 and CIP-007 and require authorization. If a particular CIP-005 or CIP-007 cyber security control cannot be implemented due to “technical infeasibility” or “per system capability”, then that unimplemented cyber security control would not be in scope for CIP-010-5 Requirement R1, nor Requirement Part 1.2 rendering the need for that language moot.

Additionally, the SDT chose to add to the phrase “that minimizes differences with the production environment” to eliminate the dependency on baseline configuration, as well as to mitigate the need for a TFE.

Rationale for Requirement R1 Part 1.3

Conforming changes to Applicable Systems (see General Considerations above).

Requirement R1 Part 1.3 is where CIP-010-4 Requirement R1 Part 1.6 now lands in CIP-010-5, with conforming changes to remove the ‘baseline configuration’ terminology and instead referring to operating systems, firmware, software, or software patches changes as the trigger for the Requirement Part.

The SDT acknowledges virtualization vendors may provide a “golden image” to clone multiple other Virtual Cyber Assets as described in the “Parent/Child Images” section above. The SDT intent is for entities that use the golden image technology to account for the software source and integrity of the golden image which covers any unmodified clones derived from it.

Rationale for Requirement R1 Part 1.4

Requirement Part 1.4 is a simplified version of the same part 1.4 in the previous version. The SDT made conforming changes to align the scope of this part with 1.1 with the phrasing “As a part of the changes authorized per Part 1.1…”.

It is important to note the SDT intent and rationale behind the wording “As a part of the change”. The rationale for that phrase is the entity, before closing out that change, will verify that the change has not adversely affected the altered cyber security controls. If the entity, as part of the post change verification, finds that it did, the entity must remediate that issue. The intent is this change not be completed until it is verified that the cyber security controls are not adversely affected.

What was 1.4.1 in the previous version required the entity to determine, prior to the change, the CIP-005 and CIP-007 controls that might be affected. With the automated remediation technology at instantiation, this is no longer possible and the SDT considered it was not the security objective. The security objective, the required behavior, is that entities ensure that changes don't adversely affect the cyber security controls by verifying them after making the change. That is now the clearly stated focus of 1.4. It is not the SDT's intent that the entity must test *every* cyber security control for *every* change, which is the rationale for the wording "of the altered cyber security controls". If an entity is installing a patch to an application on a BCS, it's not the intent that the entity verify that the domain password policy wasn't changed, however, the entity should verify the patch did not open or enable any unnecessary ports for example. The requirement part 1.4.3 from the previous version to document the results of the verification has been deleted and the SDT rationale is that is essentially a requirement to provide evidence for the actions taken to comply with the requirement part. Therefore 1.4 is now a simplified security objective to be met.

The rationale for the phrasing of "adversely affected" is simply to recognize that the desired effect of a change may be to impact a cyber security control – for example an entity may wish to change a password policy such that it requires stronger passwords than the CIP standard requires. That would not be an "adverse" change.

Requirement R2

General Considerations for Requirement R2

The scoping of Requirement R2 is an intentional subset of the scope for Requirement R1. The focus of CIP-010-5 Requirement R1 is authorizing changes that affect the security posture of those Applicable Systems as well as the logical environments that protect them. This is why R1 includes the obligation to authorize changes that alter the behavior of one or more cyber security controls that are implemented to protect the system or environment. The Applicable Systems for the R2 monitoring requirement for unauthorized changes is an intentional a subset of cyber security controls (CIP-007) to align with the Appliable Systems scope and those technical controls that have been implemented at the System or Cyber Asset level to maintain that cyber security posture.

The SDT has reworked R2 for monitoring for unauthorized changes to work better with the additional scope of R1's change management. The SDT's rationale is that all changes that should be included and authorized in a change management program may not have an automated solution for monitoring for unauthorized change and the SDT's intent is for this requirement's scope to be items that have a greater potential to for automated monitoring by technical controls, recognizing monitoring outputs (alarms, alerts, reports, logs etc.) may require manual review by the recipients to determine if the change was unauthorized and what subsequent actions, if any, may need to be taken. Therefore, the SDT tied R2 loosely to R1's scope but with a required list of seven cyber security-related categories to monitor. The SDT's intent when using the 'per system capability' language is to keep the scope of R2 to those things for which automated solutions are available and likely to monitor these areas and alert entities to changes. It should be noted the 'system' in 'per system capability' refers to the Applicable Systems for the requirement, and not the capability of the automated tool used to monitor. As a result, the 'per system capability' language does not absolve entities of the obligation to implement monitoring methods where automated solutions have not been implemented, and while potentially less ideal, manual methods to accomplish the same results where automated monitoring cannot be done remains a requirement where the Applicable System is capable of producing data related to the list of seven cyber security-related categories to monitor. The reference to manual reviews is also in the measures because the manual response actions to automated monitoring serves as supporting evidence and a means to demonstrate compliance with the final component of Part 2.1, which is to 'Document and investigate detected unauthorized changes'.

The SDT has added the term "unauthorized" into Requirement R2 Part 2.1 to focus it on the risk of unauthorized changes. Many implementations will perform this task by monitoring all changes and looking for unauthorized changes within that population. However, the SDT is allowing for a capability that may filter out authorized changes such that the entity can have methods to monitor for unauthorized changes only. The SDT also added "per system capability" in recognition that not all changes in scope can be monitored on every potential in-scope Cyber System.

This addition makes the requirement conditional if a system is incapable of monitoring a particular unauthorized change category.

The SDT has used the phrasing "that include at least one cyber security control for each of the following" in order to allow entities to monitor a primary security control if they have multiple overlapping controls. The SDT's intent is that having multiple security controls over these categories is a good and beneficial practice where possible, and entities should not be discouraged from having more than one. This phrasing's intent is to allow the entity to choose the primary control they monitor for unauthorized change. The entity may of course do more than one, but one is required.

For the seven required control categories, the SDT notes it intent as follows:

2.1.1 – The intent is to monitor for changes to the system's configuration affecting ports or services that are enabled such that they provide accessibility via routable protocols on a network interface.

2.1.2 – The SDT notes that the intent of this item is conditional – evidence for this is only required "on SCI". If there is no SCI, then no control is required. If SCI is in scope, then some control to monitor for unauthorized changes to CPU/memory sharing of VCAs (affinity rules, etc.) is required.

2.1.3 - The intent of this is the traditional monitoring of changes to executable code of the various listed types. As noted in the Measures column, the SDT intends to handle the parent/child image issues by monitoring the parent image from which temporary child images are derived. See the "Parent/Child Images" section earlier in this document for examples.

2.1.4 – The intent is to monitor for unauthorized changes to the configuration of malicious code protection methods, for example whether they have been disabled, or alerting turned off, etc. Note this is not the detection or alerting or remediation of malicious code that is covered in CIP-007; this is monitoring the configuration of your method to ensure its configured behavior has not been changed in an unauthorized manner.

2.1.5 – Similar to 2.1.4, this is not monitoring the security event log and alerting as covered in CIP-007; this is monitoring the configuration of your security event logging and alerting for unauthorized changes that would change its expected behavior (disabling it, changing what is logged, changing where alerts go, etc.)

2.1.6 – The intent of "configuration of authentication methods" is to monitor for configuration changes that affect how a system authenticates its users/processes. Examples would include password policies (not individual user passwords), configuration of multi-factor authentication, changes to Pluggable Authentication Modules (PAM) on Linux systems, etc.

2.1.7 – Along with 2.1.6 concerning how a system is configured to authenticate users, this requires a control to monitor for unauthorized changes to enabled or disabled status of accounts. For example, if a "Guest" account or a default "admin" account have been disabled on a system, monitoring for the unauthorized re-enabling of those accounts.

Requirement R3

Rationale for Requirement R3 Part 3.1

Conforming changes only to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.2

Conforming changes to Applicable Systems (see General Considerations above).

The SDT chose to remove the reliance on a "Technical Feasibility Exception" in favor of the updated term "per system capability". The SDT contends that the term still requires an entity to document the limit to the system's

capability with regards to the requirement language, while not incurring the additional documentation overhead of a TFE.

In Requirement R3 Part 3.2.1, conforming changes have been made to remove the baseline configuration dependency. Additionally, the SDT chose to add to the phrase “that minimizes differences with the production environment” to eliminate the dependency on baseline configuration.

Rationale for Requirement R3 Part 3.3

The previous language of “Prior to adding a new applicable Cyber Asset to a production environment” for the timing of performing a vulnerability assessment has an interesting “chicken or egg” problem when it comes to VCAs. This phrasing for the timing has worked well for hardware “programmable electronic devices” arriving on a loading dock or spares coming in from a warehouse that should be assessed before being physically placed “in production”. However, VCA’s aren’t shipped, they are created in the production environment from a hardware perspective. A VCA image may be created on the hypervisor, an OS installed, the appropriate applications installed, etc., but the VCA is not yet connected to its production network and instantiated in a way that it has connectivity or is performing its function. However, it is from a hardware standpoint in the “production environment” so you can’t do an assessment “prior to” that as this is where it’s created.

To solve this issue, the SDT replaced this timing phrasing with the language “Prior to becoming a new Applicable System…”. The SDT’s rationale is the requirement part requires the vulnerability assessment at a point prior to the VCA being instantiated, with the “production” connectivity it requires, to perform its function either as a part of a BES Cyber System or EACMS or PCA. As it begins to perform those functions (i.e., for an EACMS to begin controlling or monitoring electronic access), it becomes an “Applicable System” at that point – prior to that point in time the vulnerability assessment of that VCA should have taken place. The remediation VLAN technologies may perform this automatically at every instantiation. The SDT made this change so that the requirement part did not imply that VCAs had to be created elsewhere, in some other separate hardware environment, assessed, and then somehow imported. Conforming changes have been made to remove the baseline configuration dependency. The exceptions are “Like replacements or additions with a previously assessed configuration of an existing Applicable System; or CIP Exceptional Circumstances”.

Conforming changes made to Applicable Systems (see General Considerations above).

Rationale for Requirement R3 Part 3.4

Conforming changes made only to Applicable Systems (see General Considerations above).

Requirement R4

General Considerations for Requirement R4

The SDT updated Requirement R4 to include associated SCI into the scope of the required plans for Transient Cyber Assets (TCA) and Removable Media. The SDT also updated Attachment 1, such that the scope is clarified once within Requirement R4 and applies throughout Attachment 1.

The SDT corrected a perceived mismatch of control to objective by moving the control “Live operating system and software executable only from read only media;” from Part 1.3 to Part 1.4 as a better location for the control to serve the objective of the Part, which aligns with Sections 2.1 & 2.2.

The SDT also made several conforming changes to Attachment 1 for TCAs to ensure continuity in language between the measures and similar sections in CIP-003 Attachment 1.

Former Background Section from Reliability Standard CIP-010-4

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.
Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances

“Applicable Systems” Columns in Tables:

Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicability Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Technical Rationale for Reliability Standard CIP-010-4

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-010-4. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justification for CIP-010-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850[1] on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards, in which the summary on page 1 states, "…the Commission directs NERC to develop and submit modifications to the supply chain risk management Reliability Standards so that the scope of the Reliability Standards include Electronic Access Control and Monitoring Systems." In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report, Staff Report and Recommended Actions[2], to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-010-4 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-010-4 uses the following definition(s), which are cited below for reference when reading the technical rational that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1

General Considerations for Requirement R1

FERC Order 850, Paragraph 5 and Paragraph 30 directed modifications to Reliability Standard CIP-010-3 Requirement R1 to address supply chain risk management for Electronic Access Control or Monitoring Systems (EACMS) for high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards to address PACS that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems, and modifications were addressed by the 2019-03 SDT.

Rationale for Requirement R1

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

---

[1] https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf

[2] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

Requirement R1 Part 1.6 addresses directives in Order No. 850 for verifying software integrity and authenticity prior to installation of an EACMS (P. 5 and P.30), and PACS from the NERC Cyber Security Supply Chain Risk Report[3] recommendation. The objective of verifying software integrity and authenticity is to ensure that the software being installed on EACMS and PACS was not modified without the awareness of the software supplier and is not counterfeit.

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements, the SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls. Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. is consistent with the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[4].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While it might be a fair point that a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it stands to reason that a threat actor's intention to gain unauthorized electronic access to a PACS does so 1) with the knowledge of it being an initial deliberate action to facilitate undetected reconnaissance, and 2) further undetected methodical compromise and intentional harm to the BES Cyber Systems the PACS is intended to protect.

Furthermore, a precedent is set in CIP-006-6 Requirement R1 Part 1.5 that recognizes the importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter (PSP) to incident response personnel within 15 minutes of detection. This strict timeline suggests that compromised physical security poses an imminent threat to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

---

[3] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019.
https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[4] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019.
https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report, the SDT risks associated with the different aspects of both EACMS and PACS. The NERC Supply Chain Report pointed to the increased risk of the control portion of both EACMS and PACS, and the SDT considered limiting the scope of the requirements to only those EACMS and PACS that perform the control functions. However, since the current approved definitions includes both control and monitoring for EACMS and control, logging and alerting for PACS, the SDT concluded it would introduce less confusion by referring to the authoritative term. The SDT did not attempt a change in definition due to the wide spread use of both EACMS and PACS within all the standards, and did not have authorization within its SAR to modify all of those standards.

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The language for use of a testing environment for deviations from baseline configuration was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of verifying the identity of the software source and the integrity of the software obtained from the software source helps prevent the introduction of malware or counterfeit software. This reduces the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The SDT intends for Responsible Entities to provide controls for verifying the baseline elements updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2

Rationale for Requirement R2

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Baseline Monitoring

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible

Requirement R3

Rationale for Requirement R3

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Vulnerability Assessments

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4

Rationale for Requirement R4

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Transient Cyber Assets and Removable Media

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management. With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Attachment 1

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity’s responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity’s security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity’s plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Technical Rationale for Reliability Standard CIP-010-3

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-010-3 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Section 4 – Scope of Applicability of the CIP Cyber Security Standards:

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to “model” the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly.

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

Requirement R2:

The SDT’s intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible. For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media.

The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example,, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.

- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

Rationale for Requirement R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for Requirement R4:

Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.
- Requirement R4 incorporates the concepts from other CIP requirements in CIP-010-2 and CIP-007-6 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes:

All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Information Protection

Technical Rationale and Justification for Reliability Standard CIP-011-4

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-011-4 . It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-011-4 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rational that follows.

General Considerations

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-011-4 to align information protection requirements with the virtualization changes.

Requirement R1 and R2

Rationale

To enable CIP-011-4 for virtualization, the SDT added “Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part” within the Applicable Systems column of each of the Parts for Requirement R1 – Requirement R2.

Requirement R2 Part 2.1

Requirement R2 Part 2.1 is an objective level requirement focused on protecting BES Cyber System Information (BCSI) rather than ‘Cyber Assets’ and ‘storage media’ and was modified to include the currently approved Requirement R2 Part 2.2. This consolidation is necessary to enable flexibility, allowing for cryptographic erasure in scenarios where BCSI cannot be mapped to one or more disks within a virtualized storage cluster, and where BCSI is stored on Cyber Systems employing deduplication. This adjustment is also future-looking to better position CIP-011 for the enablement of cloud type scenarios where the disks are owned and/or managed by a third-party as a service to the entity for its BCSI storage, analysis, or use.

Requirement R2 Part 2.2

Requirement R2 Part 2.2 has been deleted because it was consolidated into Requirement R2 Part 2.1.

Former Background Section from Reliability Standard CIP-011-3

The section **6. Background** has been retired and removed from the Standard, and preserved by cutting and pasting as-is below.

Background

Standard CIP-011 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc.] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in its documented processes, but it must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the BES. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

“Applicable Systems” Columns in Tables: Each table has an “Applicable Systems” column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology (“NIST”) Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the “Applicable Systems” column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

Requirement R1

General Considerations for Requirement R1

None

Rationale for Modifications to Requirement R1:

Requirement R1 still specifies the need to implement one or more documented information protection program(s). The SDT does not intend that this requirement cover publicly available information, such as vendor manuals or information that is deemed to be publicly releasable. Information protection pertains to both digital and hardcopy information.

The SDT clarified the intent of protecting BCSI as opposed to protecting the BES Cyber System(s) and associated applicable systems which may contain BCSI. This was achieved by modifying the parent CIP-011-X R1 requirement language to include "for BES Cyber System Information (BCSI) pertaining to Applicable Systems".

Rationale for Modifications to Requirement R1, Part 1.1

Requirement R1, Part 1.1, is an objective level requirement focused on identifying BES Cyber System Information (BCSI). The intent of the SDT was to simplify the requirement language from CIP-011-2 Part 1.1.

Rationale for Modifications to Requirement R1, Part 1.2

Requirement R1, Part 1.2, is an objective level requirement focused on protecting and securely handling BES Cyber System Information (BCSI) in order to mitigate risks of compromising confidentiality. The reference to different states of information such as "transit" or "storage" or "use" was removed. The intent is to reduce confusion of Responsible Entities attempting to interpret controls specific to different states of information, limiting controls to said states, overlapping controls between states, and reduce confusion from an enforcement perspective. By removing this language, methods to protect BCSI becomes explicitly comprehensive.

Requirement language revisions reflect consistency with other CIP requirements.

Requirement R2

General Considerations for Requirement R2

None

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BCSI upon reuse or disposal.

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

Requirement 2 has remained unchanged. The requirements are focused more on the reuse and disposal of BCS rather than BCSI. While acknowledging that such BCS and other applicable systems may have BCSI residing on them, the original intent of the requirement is broader than addressing BCSI. This is a lifecycle issue concerning the applicable systems. CIP-002 focuses on the beginning of the BCS lifecycle but not an end. The potential end of the applicable systems lifecycle is absent from CIP-011 to reduce confusion with reuse and disposal of BCSI. The 2019 BCSI Access Management project did not include modification of CIP-002 in the scope of the SAR. This concern has been communicated for future evaluation.

Technical Rationale for Reliability Standard CIP-011-2

This section contains a "cut and paste" of the former Guidelines and Technical Basis (GTB) as-is of from CIP-011-2 standard to preserve any historical references. No modifications have been made.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5.1's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity’s program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use. This includes information that may be stored on Transient Cyber Assets or Removable Media.

The entity’s written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity’s Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].

Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Requirement R1:

The SDT’s intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Rationale for Requirement R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security — Supply Chain Risk Management

Technical Rationale and Justification for Reliability Standard CIP-013-3

April 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Technical Rationale for Reliability Standard CIP-013-3

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-3. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. This Technical Rationale and Justifications for CIP-013-3 is not a Reliability Standard and should not be considered mandatory and enforceable.

Updates to this document now include the Project 2016-02 – Modifications to CIP Standards Drafting Team's (SDT's) intent in drafting changes to the requirements.

Background

The Version 5 Transition advisory Group (V5TAG), which consists of representatives from NERC, Regional Entities, and industry stakeholders, was formed to issue guidance regarding possible methods to achieve compliance with the CIP V5 standards and to support industry's implementation activities. During the course of the V5TAG's activities, the V5TAG identified certain issues with the CIP Reliability Standards that were more appropriately addressed by a standard drafting team (SDT). The V5TAG developed the V5TAG Transfer Document to explain the issues and recommend that they be considered in future development activity. As Project 2016-02 was formed to address the directives in FERC Order 822 issued on January 21, 2016, that team also received the V5TAG issues as part of its Standard Authorization Request (SAR).

One of the areas of issue was virtualization. The V5TAG Transfer document said, "The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration. The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies."

New and Modified Terms and Applicability

This standard uses new or modified terms and contains new or modified exemptions in Section 4 Applicability. The rationale for this global content can be found in "CIP Definitions and Exemptions Technical Rationale" document for reference when reading the technical rationale that follows.

Requirement R1

Rationale

The Project 2016-02 SDT made conforming changes to Reliability Standard CIP-013-3 to align supply chain risk management requirements with the virtualization changes.

To enable CIP-013-3 for virtualization, the SDT added "and Shared Cyber Infrastructure (SCI)" to the parent Requirement R1. Additionally, the SDT simplified the applicability in Requirement R1 Parts 1.1 and 1.2 by replacing the long list of applicable systems with a reference to the list in the parent Requirement R1 through the use of this language, "applicable systems listed in Requirement R1". Note: Because CIP-013-3 does not contain the "Table" construct with an "Applicable Systems" column, this term is not defined within Section 4 Applicability; Therefore, where used, "applicable systems" is intentionally not capitalized within the requirement language of Requirement R1 Parts 1.1 and 1.2.

Technical Rationale for Reliability Standard CIP-013-2

This section contains a "cut and paste" of the Technical Rationale for CIP-013-2 standard to preserve any historical references.

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-013-2. It provides stakeholders and the ERO Enterprise with an understanding of the technology and technical requirements in the Reliability Standard. It also contains information on Project 2019-03 Cyber Security Supply Chain Risks Standard Drafting Team's (SDT's) intent in drafting the requirements. This Technical Rationale and Justification for CIP-013-2 is not a Reliability Standard and should not be considered mandatory and enforceable.

The Federal Energy Regulatory Commission (the Commission) issued Order No. 850 on October 18, 2018, calling for modifications to the Supply Chain Suite of Standards to address Electronic Access Control or Monitoring Systems (EACMS), specifically those systems that provide electronic access control or monitoring to high and medium impact BES Cyber Systems. In addition, NERC also recommended revising the Supply Chain Standards in its May 17, 2019 NERC Cyber Security Supply Chain Risk Report to address Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems.

The Project 2019-03 SDT drafted Reliability Standard CIP-013-2 to require responsible entities to meet the directives set forth in the Commission's Order No. 850 and the NERC Cyber Security Supply Chain Risk Report.

New and Modified Terms Used on NERC Reliability Standards

CIP-013-2 uses the following definition(s), which are cited below for reference when reading the technical rationale that follows.

Proposed Modified Terms: None

Proposed New Terms: None

Requirement R1 and R2

General Considerations for Requirements R1 and R2

The Requirement addresses Order No. 829 directives for entities to develop and implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems. FERC Order 850, Paragraph 5 and Paragraph 30, directs modifications to Reliability Standards to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Supply Chain Risk Management Standards. In addition, NERC also recommended revising the Supply Chain Standards in its May 17,

2019 NERC Cyber Security Supply Chain Risk Report [1](Chapter 3, pages 12-15) to address PACS that provide physical access control to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Due to the nature of PACS and the potential need for physical presence, the SDT conducted extensive dialogue and consideration for the addition of PACS to the requirements. The SDT concluded the risk posed to BES reliability by a compromised, misused, degraded, or unavailable PACS warrants the inclusion of PACS as an applicable Cyber Asset category for supply chain risk management controls.

Further, the inclusion of PACS:

1. addresses the Commission's remaining concern stated in FERC Order No. 850 P 6. that, "…the exclusion of these components may leave a gap in the supply chain risk management Reliability Standards.",
2. addresses the expectations of FERC Order No. 850 P 24. "…to direct that NERC evaluate the cybersecurity supply chain risks presented by PACS and PCAs in the study of cybersecurity supply chain risks directed by the NERC BOT in its resolutions of August 10, 2017.", and
3. directly aligns with NERC's recommendation to include PACS as documented in NERC's final report on "*Cyber Security Supply Chain Risks"*[2].

In further support of the SDT's decision to include PACS, as cited on page 4 of NERC's final report on "*Cyber Security Supply Chain Risks"*, "The NERC CIP Reliability Standards provide a risk-based, defense-in-depth approach to securing the BES against cyber and physical security threats." While this statement appears in the context of EACMS, it acknowledges physical security threats equally; therefore, the concept is transferable and applicable to PACS, which serve as an integral component to a strategy involving layers of detective and preventive security controls. PACS are intended to manage physical access to BES Cyber Systems in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES and are implemented with that specific intention to protect the BES Cyber System.

Additionally, NERC states on page 15 of their final report on "*Cyber Security Supply Chain Risks"* that, "In addition, a threat actor must be physically present at the facility in order to exploit the vulnerability created by a compromised PACS system. A threat actor may also need to bypass several physical access or monitoring controls that have not been compromised in order to gain access." While a cyber-compromised PACSs may not in and of itself represent an immediate 15-minute adverse impact to the reliability of the BES, it could demonstrate a threat Actor's intention to gain fully unauthorized electronic access. With electronic access to the PACS an initial deliberate action to facilitate reconnaissance and intentional harm to the BES Cyber Systems.

Furthermore, there is precedent set in CIP-006-6 Requirement R1 Part 1.5 that speaks to a recognized importance of PACS, its functions, and the timeliness of information provided by these systems by requiring issuance of an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to incident response personnel within 15 minutes of detection. This strict timeline suggests imminent threat that compromised physical security poses to the associated BES Cyber System and the reliable operation of the BES Facilities it serves.

---

[1] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

[2] NERC, "Cyber Security Supply Chain Risks, Staff Report and Recommended Actions", May 17, 2019. https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

The SDT agrees that NERC correctly refers to various Reliability Standards that mitigate certain security risks relating to PACS; however, the SDT asserts that these existing requirements do not address risk associated to the supply chain and therefore do not sufficiently mitigate that risk.

An additional aspect of the NERC Supply Chain Report the SDT considered was around the risk associated with the different aspects of both EACMS and PACS. While both types of systems, under the current definitions, have various functional activities they perform, the NERC Supply Chain Report pointed to the increased risk of the control function. The SDT considered limiting the scope of the requirements to only control functions, however, chose to stay with the currently approved definitions of both EACMS and PACS. The SDT concluded staying with approved definitions would introduce less confusion. Additionally an attempt to change the EACMS and PACS definitions was outside the 2019-03 SAR.

Rational for Requirement 1 and Requirement 2

Requirement R1 Part 1.1 addresses the directive in Order No. 829 (P.56) and Order 850 (P.5) for identification and documentation of cyber security risks in the planning and development processes related to the procurement of medium and high impact BES Cyber Systems, and their associated EACMS and PACS. The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

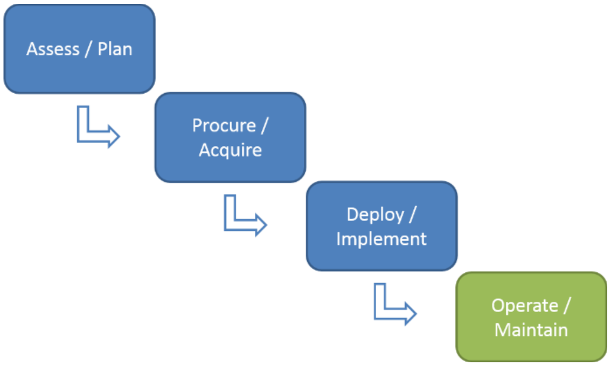
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The use of remote access in Part 1.2.6 includes vendor-initiated authenticated remote connections and system to system remote connections for EACMS and PACS; and vendor-initiated IRA and system to system access to BCS and PCAs.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R3

General Considerations for Requirement R3

The requirement addresses Order No. 829 directives for entities periodically to reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Technical Rational for Reliability Standard CIP-013-1

This section contains a "cut and paste" of the Technical Rationale components of the former Guidelines and Technical Basis (GTB) as-is of from CIP-013-1 standard to preserve any historical references. Similarly, former GTB content providing compliance guidance can be found in a separate Implementation Guidance document for this standard.

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;

(2) Vendor remote access;

(3) Information system planning; and

(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

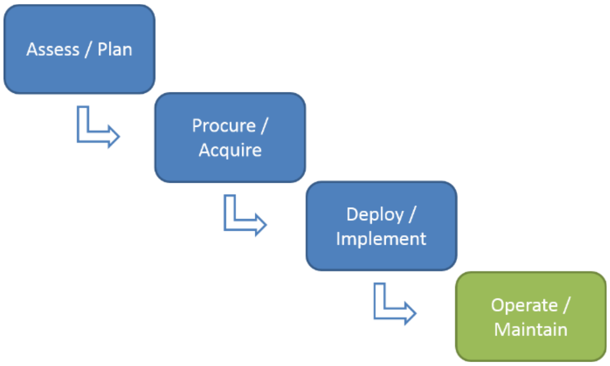
Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-02 Modifications to CIP Standards

This document provides the standard drafting team's (SDT's) justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in the project-related standards. Each requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the Electric Reliability Organizations (ERO) Sanction Guidelines. The SDT applied the following NERC criteria and FERC Guidelines when developing the VRFs and VSLs for the requirements.

The VRFs and VSLs can be found within each Reliability Standard. This document provides justification for Reliability Standards with more substantive changes to the VRFs and VSLs, not justification for the Reliability Standards without substantive changes or only conforming changes to VRFs and VSLs from the last FERC-approved versions.

- CIP-002-7: There were no changes to VRFs and only conforming or non-substantive changes to VSLs.
- CIP-003-10: There were no changes to VRFs and justification for VSLs is provided below.
- CIP-004-8: There were no changes to VRFs and justification for VSLs is provided below.
- CIP-005-8: There were no changes to VRFs and justification for VSLs is provided below.
- CIP-006-7: There were no changes to VRFs and only conforming changes to VSLs.
- CIP-007-7: There were no changes to VRFs and justification for VSLs is provided below.
- CIP-008-7: There were no changes to VRFs and no substantive changes to VSLs.
- CIP-010-5: There were no changes to VRFs and justification for VSLs is provided below.
- CIP-011-4: There were no changes to VRFs and no substantive changes to VSLs.
- CIP-013-3: There were no changes to VRFs and no substantive changes to VSLs.

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. However, violation of a medium risk requirement is unlikely to lead to Bulk Electric System instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management

- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard

FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards

FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level

Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation

Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple “degrees” of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC’s overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a “binary” type requirement must be a “Severe” VSL.
Do not use ambiguous terms such as “minor” and “significant” to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on a Single Violation, Not on a Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the “default” for penalty calculations.

VSL justification for CIP-003-10 Requirements R1, R2, R3, and R4

The VSLs were revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-003-10, Requirements R1, R2, R3, and R4	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-004-8 Requirement R1

The VSL did not substantively change from the previously FERC approved Reliability Standard CIP-004-7.

VSL justification for CIP-004-8 Requirements R2, R3, R5 and R6

The VSLs were revised for readability by deleting the deliverable language associated with certain violations.

VSL justification for CIP-004-8 Requirement R4

The VSLs were revised from the previously FERC approved Reliability Standard CIP-004-7 to add a moderate VSL and a high VSL to account for failing to authorize electronic access based on need for one or two individuals, respectively, to be consistent with the VSL in Requirement R5 and to align with FERC VSL G2a.

VSL Justifications for CIP-004-8, Requirements R2, R3, R4, R5 and R6	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-004-8, Requirements R2, R3, R4, R5 and R6	
Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-005-8 Requirement R1

The VSL changed from the previously FERC approved Reliability Standard CIP-005-7:

1. To add severe VSLs to conform with the addition of SCI to Appliable Systems;
2. To accommodate for the modified requirement part language to enable for virtualization through protections for Management Interfaces, routable protocol communications, and the exclusion time sensitive communications of Protection Systems;
3. To account for the consolidation of the previously FERC approved CIP-006-6 Requirement R1 Part 1.10 into the final draft of CIP-005-8 Requirement R1 Part 1.6; and
4. Were also revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-005-8, Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-005-8, Requirement R1	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-005-8 Requirement R2

The VSL changed from the previously FERC approved Reliability Standard CIP-005-7.

1. To add severe VSLs to conform with the addition of SCI to Appliable Systems;
2. To accommodate for the modified requirement part language to prevent Intermediate Systems from sharing CPU resources or memory resources with any part of a high or medium impact BCS, and to ensure routable protocol communications from and Intermediate System to a high or medium BCS went through an ESP; and
3. Were revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-005-8, Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-005-8, Requirement R2	
for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-005-8 Requirement R3

The VSL changed from the previously FERC approved Reliability Standard CIP-005-7:

1. To add severe VSLs to conform with the addition of SCI to Appliable Systems; and
2. Were also revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-005-8, Requirement R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity

VSL Justifications for CIP-005-8, Requirement R3	
Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-007-7 Requirement R1

The VSL changed from the previously FERC approved Reliability Standard CIP-007-6:

1. To add lower and high VSLs to align with FERC VSL G2a;
2. To accommodate for the modified requirement part language to prevent sharing of CPU resources or memory resources between VCAs that are, or are associated with, a Medium or High Impact BCS, and VCAs that are not, or are not associated with a Medium or High Impact BCS;
3. To account for network accessible services; and
4. Were revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-007-7 Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-007-7 Requirement R1	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-007-7 Requirement R2

The VSLs were revised for readability by deleting the deliverable language associated with certain violations and to assure consistency in language by qualifying the term ‘patches’ with ‘cyber security’.

VSL justification for CIP-007-7 Requirements R3 and R4

The VSLs were revised for readability by deleting the deliverable language associated with certain violations.

VSL justification for CIP-007-7 Requirement R5

The VSLs were revised for readability by deleting the deliverable language associated with certain violations and updated to accommodate for the replacement of technical feasibility exception language with per cyber system capability language in certain requirement parts.

VSL Justifications for CIP-007-7 Requirements R2, R3, R4 and R5	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-007-7 Requirements R2, R3, R4 and R5	
Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-010-5 Requirement R1

The VSL changed from the previously FERC approved Reliability Standard CIP-010-4:

1. To add moderate VSLs to conform with the addition of SCI to Appliable Systems; and
2. To accommodate for the consolidated requirement parts and language to enable for virtualization through the shift from a prescriptive baseline to an objective level requirement for processes to authorize changes that alter the behavior of cyber security controls serving the requirement parts of CIP-005 and CIP-007.

VSL Justifications for CIP-010-5 Requirement R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VSL Justifications for CIP-010-5 Requirement R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-010-5 Requirement R2
The VSL changed from the previously FERC approved Reliability Standard CIP-010-4 to align with FERC VSL G2a:

1. By adding a moderate, and a high VSL to account for failing to include in documented and implemented configuration monitoring process(es) ‘one or two’, or ‘three or four’, of the required Parts 2.1.1 through 2.1.7 for Applicable Systems, respectively; and modifying the severe VSL for failing to include 5 or more of the required Parts 2.1.1 through 2.1.7 for Applicable Systems in documented and implemented configuration monitoring process(es).
2. By adding a lower, moderate, and a high VSL to account for failing to monitor within 35 calendar days and exceeding the required cadence by monitoring for 36 to 69 calendar days, 70 to 104 calendar days, 105 to 139 calendar days, respectively; and modifying the severe VSL for failing to monitor for 140 calendar days or more as required by Part 2.1.

VSL Justifications for CIP-010-5 Requirement R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-010-5 Requirement R2	
for "Binary" Requirements Is Not Consistent <u>Guideline 2b</u>: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

VSL justification for CIP-010-5 Requirements R3 and R4
The VSLs were revised for readability by deleting the deliverable language associated with certain violations.

VSL Justifications for CIP-010-5 Requirements R3 and R4	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-010-5 Requirements R3 and R4	
Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Each VSL is based on a single violation and not cumulative violations.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-002-7 — Cyber Security — BES Cyber System Categorization

This section to be completed by the Compliance Enforcement Authority.

Audit ID: Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity: Registered name of entity being audited
NCR Number: NCRnnnnn
Compliance Enforcement Authority: Region or NERC performing audit
Compliance Assessment Date(s)[2]: Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method: [On-site Audit | Off-site Audit | Spot Check]
Names of Auditors: Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X		X			X	X		
R2	X	X	X	X		X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

---

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of Parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** RAS that support the reliable operation of the BES; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above*.

- **1.1.** Identify each of the high impact BCS according to Attachment 1, Section 1, if any, at each asset;
- **1.2.** Identify each of the medium impact BCS according to Attachment 1, Section 2, if any, at each asset; and
- **1.3.** Identify each asset that contains a low impact BCS according to Attachment 1, Section 3, if any (a discrete list of low impact BCS is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1.

* See the full text of CIP-002-7 for this reference.

Registered Entity Response (Required):
Question 1: Do you share compliance responsibility for this Requirement with another Responsible Entity?
☐ Yes ☐ No
For example, is any BCS located at a shared facility?
If "Yes," list the following for each asset for which compliance responsibility is shared:

1. Asset name or designation.
2. Formal agreement or other document describing the shared compliance responsibility, if any.
3. Other information regarding the shared compliance responsibility which may be useful to the audit team in determining the appropriate audit scope and approach for the asset.

Note: A separate spreadsheet or other document may be used to provide all or part of this information. If so, provide the document reference below.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-002-7, R1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has a process to identify each high impact BCS, each medium impact BCS, and each asset that contains a low impact BCS.
	Verify the above process considers all of the following: i. Control Centers and backup Control Centers; ii. Transmission stations and substations; iii. Generation resources; iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v. RAS that support the reliable operation of the BES; and vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 of the Standard.
	Verify the Responsible Entity has identified each of the high impact BCS according to Attachment 1, Section 1, if any, at each asset.
	Verify the Responsible Entity has identified each of the medium impact BCS according to Attachment 1, Section 2, if any, at each asset.
	Verify the Responsible Entity has identified each asset that contains a low impact BCS according to Attachment 1, Section 3, if any.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

Registered Entity Response:

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-002-7, R2

This section to be completed by the Compliance Enforcement Authority

	Verify the reviews of the identifications in Requirement R1 have occurred at least once every 15 calendar months.
	Verify the approvals by the CIP Senior Manager or delegate of the identifications in Requirement R1 have occurred at least once every 15 calendar months.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-002-7 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

FERC Order No. 822

Attachment 1 – Impact Rating Criteria

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. **High impact rating**
   Each BCS used by and located at any of the following:

   1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

   1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

   1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

   1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. **Medium impact rating**
   Each BCS, not included in Section 1 above, associated with any of the following:

   2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

   2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BCS that meet this criterion are each discrete shared BCS that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

   2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each RAS, or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in high impact rating above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in high impact rating, above.

2.13. Each Control Center or backup Control Center, not already included in high impact rating above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low impact rating

BCS not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. RAS that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFT1v0	02/28/2024		Initial Draft

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-003-10 – Cyber Security — Security Management Controls

This section to be completed by the Compliance Enforcement Authority.

Audit ID: Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity: Registered name of entity being audited
NCR Number: NCRnnnnn
Compliance Enforcement Authority: Region or NERC performing audit
Compliance Assessment Date(s)[2]: Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method: [On-site Audit | Off-site Audit | Spot Check]
Names of Auditors: Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		
R3	X	*	X	X		X			X	X		
R4	X	*	X	X		X			X	X		

* CIP-003-10 is only applicable to DPs that own certain UFLS, UVLS, RAS, Protection Systems, or Cranking Paths. See CIP-003-10 Section 4, Applicability, for details.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

---

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request additional evidence from the registered entity that is not included in this RSAW. This RSAW may include excerpts from FERC Orders and other regulatory references which are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			
R4			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1.** For its high impact and medium impact (BCS), if any:
  - **1.1.1.** Personnel and training (CIP-004);
  - **1.1.2.** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
  - **1.1.3.** Physical security of BCS (CIP-006);
  - **1.1.4.** System security management (CIP-007);
  - **1.1.5.** Incident reporting and response planning (CIP-008);
  - **1.1.6.** Recovery plans for BCS (CIP-009);
  - **1.1.7.** Configuration change management and vulnerability assessments (CIP-010);
  - **1.1.8.** Information protection (CIP-011); and
  - **1.1.9.** Declaring and responding to CIP Exceptional Circumstances.
- **1.2.** For its assets identified in CIP-002 containing low impact BCS, if any:
  - **1.2.1.** Cyber security awareness;
  - **1.2.2.** Physical security controls;
  - **1.2.3.** Electronic access controls;
  - **1.2.4.** Cyber Security Incident response;
  - **1.2.5.** Transient Cyber Assets (TCA) and Removable Media malicious code risk mitigation;
  - **1.**2.6 Vendor electronic remote access security controls; and
  - **1.2.7.** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-003-10, R1

This section to be completed by the Compliance Enforcement Authority

	For its high impact and medium impact BCS, if any, verify the Responsible Entity has documented one or more cyber security policies that collectively address the following topics: 1. Personnel and training (CIP-004); 2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access; 3. Physical security of BCS (CIP-006); 4. System security management (CIP-007); 5. Incident reporting and response planning (CIP-008); 6. Recovery plans for BCS (CIP-009); 7. Configuration change management and vulnerability assessments (CIP-010); 8. Information protection (CIP-011); and 9. Declaring and responding to CIP Exceptional Circumstances.
	For its assets identified in CIP-002 containing low impact BCS, if any, verify the Responsible Entity has documented one or more cyber security policies that collectively address the following topics: 1. Cyber security awareness; 2. Physical security controls; 3. Electronic access controls; 4. Cyber Security Incident response; 5. TCA and Removable Media malicious code risk mitigation; 6. Vendor electronic remote access security controls; and 7. Declaring and responding to CIP Exceptional Circumstances.
	Verify each policy used to meet this Requirement has been reviewed at least once every 15 calendar months.
	Verify the CIP Senior Manager has approved each policy used to meet this Requirement at least once every 15 calendar months.
	Verify the Responsible Entity has achieved the security objective of instituting cyber security policies that will preserve the availability, integrity, and confidentiality of systems that support the reliable operation of the BES.
Note to Auditor: Per Attachment 1, “Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.”	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BCS shall implement one or more documented cyber security plan(s) for its low impact BCS, and Shared Cyber Infrastructure (SCI) that supports a low impact BCS, that include the sections in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BCS or their BES Cyber Assets (BCA) is not required. Lists of authorized users are not required.

M2. Evidence shall include each of the documented cyber security plan(s) that collectively include each of the sections in Attachment 1 and additional evidence to demonstrate implementation of the cyber security plan(s). Additional examples of evidence per section are located in Attachment 2.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-003-10, R2

This section to be completed by the Compliance Enforcement Authority

	Attachment 1, Section 1 For each asset containing a low impact BCS, verify that the Responsible Entity has documented a plan to reinforce cyber security practices (which may include associated physical security practices) at least once every 15 calendar months.
	Attachment 1, Section 1 For each asset containing a low impact BCS, verify that the Responsible Entity has implemented its plan to reinforce cyber security practices (which may include associated physical security practices) at least once every 15 calendar months.
	Attachment 1, Section 1 For each asset containing a low impact BCS, verify that the Responsible Entity has achieved the security objective of ensuring personnel with access to low impact BCS remain aware of cyber security practices.
	Attachment 1, Section 2 For each asset containing a low impact BCS, verify that the Responsible Entity has documented a plan to control physical access, based on need as determined by the Responsible Entity, to: 1. The asset or the locations of the low impact BCS within the asset; and 2. The Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.
	Attachment 1, Section 2 For each asset containing a low impact BCS, verify that the Responsible Entity has implemented its plan to control physical access.
	Attachment 1, Section 2 For each asset containing a low impact BCS, verify that the Responsible Entity has achieved the security objective of controlling physical access to: 1. The asset or the locations of the low impact BCS within the asset; and 2. The Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.
	Attachment 1, Section 3.1 For each asset containing a low impact BCS, verify that the Responsible Entity has documented a plan to control inbound and outbound electronic access, based on need as determined by the Responsible Entity, for any communications that are: 1. Between a low impact BCS; or an SCI that supports a low impact BCS; and a Cyber System(s) outside the asset containing: the low impact BCS(s); or the SCI that supports a low impact BCS. 2. Using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that supports a low impact BCS; and 3. Not used for time-sensitive communications of Protection Systems.
	Attachment 1, Section 3.1 For each asset containing a low impact BCS, verify that the Responsible Entity has implemented its plan to control electronic access.

	Attachment 1, Section 3.1 For each asset containing a low impact BCS, verify that the Responsible Entity has achieved the security objective of permitting only necessary inbound and outbound access to its low impact BCS.
	Attachment 1, Section 3.2 For each asset containing a low impact BCS, verify that the Responsible Entity has documented a plan to authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.
	Attachment 1, Section 3.2 For each asset containing a low impact BCS, verify that the Responsible Entity has implemented the plan to authenticate Dial-up Connectivity.
	Attachment 1, Section 3.2 For each asset containing a low impact BCS, verify that the Responsible Entity has achieved the security objective of authenticating all Dial-up Connectivity, per system capability, where such connectivity permits access to its low impact BCS or SCI that supports a low impact BCS.
	Attachment 1, Section 4 For each asset containing a low impact BCS, verify that the Responsible Entity has documented one or more Cyber Security Incident response plan(s) that include: 1. Identification, classification, and response to Cyber Security Incidents; 2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law; 3. Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals; 4. Incident handling for Cyber Security Incidents; 5. Testing each Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and 6. Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.
	Attachment 1, Section 4 For each asset containing a low impact BCS, if the Responsible Entity responded to a Cyber Security Incident, verify the Responsible Entity implemented the Cyber Security Incident response plan.
	Attachment 1, Section 4.5 Verify the Responsible Entity tested each Cyber Security Incident response plan at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident.
	Attachment 1, Section 4.6

	Verify the Responsible Entity updated each Cyber Security Incident response plan, if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.
	Attachment 1, Section 4 Verify the Responsible Entity is prepared to achieve the security objective of minimizing the adverse impact to the BES of a possible Cyber Security Incident affecting low impact BCS.
	Attachment 1, Section 5.1, 5.2, 5.2.1 Verify the Responsible Entity has documented one or more plans to mitigate the risk of the introduction of malicious code to low impact BCS through the use of TCA.
	Attachment 1, Section 5.1, 5.2, 5.2.1 Verify the Responsible Entity has implemented its plans to mitigate the risk of the introduction of malicious code to low impact BCS through the use of TCA.
	Attachment 1, Section 5.1, 5.2, 5.2.1 Verify the Responsible Entity has achieved the objective of mitigating the risk of the introduction of malicious code to low impact BCS through the use of TCA.
	Attachment 1, Section 5.2.2 For any method used pursuant to 5.2.1, verify the Responsible Entity has determined whether any additional mitigation actions are necessary and has implemented such actions prior to connecting the TCA.
	Attachment 1, Section 5.3.1 Verify the Responsible Entity has documented one or more plans to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS.
	Attachment 1, Section 5.3.2 Verify the Responsible Entity has documented one or more plans to mitigate the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.
	Attachment 1, Section 5.3 Verify the Responsible Entity has implemented its plans to mitigate the risk of the introduction of malicious code to low impact BCS or SCI that supports a low impact BCS through the use of Removable Media.
	Attachment 1, Section 5.3 Verify the Responsible Entity has achieved the objective of mitigating the risk of the introduction of malicious code to low impact BCS or SCI that supports a low impact BCS through the use of Removable Media.
Note to Auditor: Attachment 1, Section 3	

1. For each asset identified as containing a low impact BCS per CIP-002, the list of assets should identify those assets that have routable protocol communications between low impact BCS; or an SCI that supports a low impact BCS and a Cyber System(s) outside the asset containing: the low impact BCS(s); or the SCI that supports a low impact BCS when entering or leaving the asset and not used for time-sensitive protection or time-sensitive control functions.
    a. For these identified assets, obtain as evidence the devices used to control electronic access and the low impact BCS for which they control access.
2. For each asset identified as containing a low impact BCS per CIP-002, the Responsible Entity has an obligation to determine the necessary inbound and outbound routable protocol communications between low impact BCS and SCI that supports a low impact BCS outside the asset containing: the low impact BCS when entering or leaving the asset and not used for time-sensitive protection or time-sensitive control functions. The Responsible Entity must be able to provide a technically sound explanation as to how its electronic access permissions and controls are consistent with the security objective of permitting only necessary inbound and outbound access to low impact BCS.
3. The audit team should assess the effectiveness of the Responsible Entity's electronic access control plan as well as the Responsible Entity's adherence to its electronic access control plan.
4. For the inbound and outbound communications that the Responsible Entity has determined to be necessary, the Responsible Entity must identify the electronic access controls used to effectively control access to and from the low impact BCS.

Attachment 1, Section 5

1. The means of verifying the mitigation of the introduction of malicious code to a low impact BCS differs depending on whether a TCA is managed by the Responsible Entity in an ongoing or an on-demand manner. The verification for a TCA managed in an ongoing manner focuses on the process of preventing malware from being introduced to the TCA. The verification for a TCA managed in an on-demand manner focuses on the process used to ensure the TCA may be safely used in a low impact BCS environment prior to such use. If the TCA is managed in both an ongoing and an on-demand manner, then both verification techniques should be employed.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-003-10, R3

This section to be completed by the Compliance Enforcement Authority

	Verify the CIP Senior Manager has been identified by name.
	Verify that any changes made to the CIP Senior Manager were dated and documented within 30 calendar days of the change.
	Verify the CIP Senior Manager is a single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-003-10, R4

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented a process to delegate authority, unless no delegations are used.
	Verify that all delegates have been identified by name or title.
	Verify that the delegation of authority includes the specific action delegated.
	Verify specific actions delegated by the CIP Senior Manager are allowed by the CIP Standards.
	Verify that the dates for all delegations have been recorded.
	Verify that the CIP Senior Manager approved all delegations.

☐	Verify that any changes made to delegations were dated and documented within 30 days of the change.

Note to Auditor:

Delegations of the CIP Senior Manager’s authority are permitted for the required approvals in CIP-002-7.1, Requirement R2, CIP-007-7, Requirement R2, Part 2.4, and CIP-013-3 R3.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-003-10 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Standards”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

Attachment 1

Required Sections for Cyber Security Plan(s)

Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.

Responsible Entities with multiple-impact BCS ratings can utilize policies, procedures, and processes for their high or medium impact BCS to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.

Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).

Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BCS within the asset, and (2) the Cyber Asset(s) or VCA, as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

Section 3. Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to:

3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:

i. Between:

- a low impact BCS; or
- An SCI that supports a low impact BCS

and a Cyber System(s) outside the asset containing:

- the low impact BCS(s); or
- the SCI that supports a low impact BCS;

ii. using a routable protocol when entering or leaving the asset containing the low impact BCS or SCI that a low impact BCS; and

iii. not used for time-sensitive communications of Protection Systems.

3.2 Authenticate all Dial-up Connectivity, if any, that provides access to low impact BCS or SCI that supports a low impact BCS, per system capability.

Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:

4.1 Identification, classification, and response to Cyber Security Incidents;

4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Information Sharing and Analysis Center (E-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation: Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more plan(s) to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BCS through the use of TCA or Removable Media. The plan(s) shall include:

5.1 For TCA managed by the Responsible Entity, if any, the use of one or a combination of the following in an ongoing or on-demand manner (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

5.2 For TCA managed by a party other than the Responsible Entity, if any:

5.2.1 Use one or a combination of the following prior to connecting (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the introduction of malicious code.

5.2.2 For any method used pursuant to 5.2.1, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

5.3 For Removable Media, the use of each of the following:

5.3.1 Method(s) to detect malicious code on Removable Media using a Cyber Asset or VCA other than a BCS or SCI that supports a low impact BCS; and

5.3.2 Mitigation of the threat of detected malicious code on the Removable Media prior to connecting Removable Media to a low impact BCS or SCI that supports a low impact BCS.

Section 6. Vendor Electronic Remote Access Security Controls: For assets containing low impact BES Cyber System(s) identified pursuant to CIP-002, that allow vendor electronic remote access, the Responsible Entity shall implement a process to mitigate risks associated with vendor electronic remote access, where such access has been established under Section 3.1. These processes shall include:

6.1 One or more method(s) for determining vendor electronic remote access;

6.2 One or more method(s) for disabling vendor electronic remote access, and

6.3 One or more method(s) for detecting known or suspected inbound and outbound malicious communications for vendor electronic remote access.

Attachment 2

Examples of Evidence for Cyber Security Plan(s)

Section 1. Cyber Security Awareness: An example of evidence for Section 1 may include, but is not limited to, documentation that the reinforcement of cyber security practices occurred at least once every 15 calendar months. The evidence could be documentation through one or more of the following methods:

- Direct communications (for example, e-mails, memos, or computer-based training);
- Indirect communications (for example, posters, intranet, or brochures); or
- Management support and reinforcement (for example, presentations or meetings).

Section 2. Physical Security Controls: Examples of evidence for Section 2 may include, but are not limited to:

- Documentation of the selected access control(s) (e.g., card key, locks, perimeter controls), monitoring controls (e.g., alarm systems, human observation), or other operational, procedural, or technical physical security controls that control physical access to both:

  a. The asset, if any, or the locations of the low impact BCS within the asset; and

  b. The Cyber System(s) specified by the Responsible Entity that provide(s) electronic access controls implemented for Attachment 1, Section 3.1, if any.

Section 3. Electronic Access Controls: Examples of evidence for Section 3 may include, but are not limited to:

1. Documentation showing that at each asset or group of assets, the routable protocol communication as outlined in Section 3 is restricted by electronic access controls to permit only inbound and outbound electronic access that the Responsible Entity deems necessary, except where an entity provides rationale that communications are used for time-sensitive communications of Protection Systems. Examples of such documentation may include, but are not limited to representative diagrams that illustrate control of inbound and outbound communication(s) or lists of implemented electronic access controls (e.g., access control lists restricting IP addresses, ports, or services; implementing unidirectional gateways).

2. Documentation of authentication for Dial-up Connectivity (e.g., dial out only to a preprogrammed number to deliver data, dial-back modems, modems that must be remotely controlled by the control center or control room, or access control on the BCS).

Section 4. Cyber Security Incident Response: An example of evidence for Section 4 may include, but is not limited to, dated documentation, such as policies, procedures, or process documents of one or more Cyber Security Incident response plan(s) developed either by asset or group of assets that include the following processes:

1. to identify, classify, and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and for notifying the Electricity Information Sharing and Analysis Center (E-ISAC);
2. to identify and document the roles and responsibilities for Cyber Security Incident response by groups or individuals (e.g., initiating, documenting, monitoring, reporting, etc.);
3. for incident handling of a Cyber Security Incident (e.g., containment, eradication, or recovery/incident resolution);
4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and
5. to update, as needed, Cyber Security Incident response plan(s) within 180 calendar days after completion of a test or actual Reportable Cyber Security Incident.

Section 5. TCA and Removable Media Malicious Code Risk Mitigation:

1. Examples of evidence for Section 5.1 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.
2. Examples of evidence for Section 5.2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity’s acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

   Examples of evidence for Attachment 1, Section 5.2.2 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigation is necessary and has been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

3. Examples of evidence for Section 5.3.1 may include, but are not limited to, documented process(es) of the method(s) used to detect malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Examples of evidence for Section 5.3.2 may include, but are not limited to, documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and the mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Section 6. Vendor Electronic Remote Access Security Controls: Examples of evidence showing the implementation of the process for Section 6 may include, but are not limited to:

1. For Section 6.1, documentation showing:
    - steps to preauthorize access;
    - alerts generated by vendor log on;
    - session monitoring;
    - security information management logging alerts;
    - time-of-need session initiation;
    - session recording
    - system logs; or
    - other operational, procedural, or technical controls.

2. For Section 6.2, documentation showing:
    - disabling inbound and/or outbound hardware or software ports, services, or access permissions on applications, firewall, IDS/IPS, router, switch, VPN, Remote Desktop, remote control, or other hardware or software used for providing vendor electronic remote access;
    - disabling communications protocols (such as IP) used for systems which establish and/or maintain vendor electronic remote access;
    - removing physical layer connectivity (e.g., disconnect an Ethernet cable, power down equipment);
    - administrative control documentation listing the methods, steps, or systems used to disable vendor electronic remote access; or
      other operational, procedural, or technical controls

3. For Section 6.3, documentation showing implementation of processes or technologies which have the ability to detect malicious communications such as:
    - Anti-malware technologies;
    - Intrusion Detection System (IDS)/Intrusion Prevention System (IPS);
    - automated or manual log reviews;

- alerting; or
- other operational, procedural, or technical controls.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFT1v0	02/28/2024		Initial Draft

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-004-8 – Cyber Security – Personnel & Training

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X		X			X	X		
R2	X	X	X	X		X			X	X		
R3	X	X	X	X		X			X	X		
R4	X	X	X	X		X			X	X		
R5	X	X	X	X		X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

---

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			
R4			
R5			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-004-8 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS Medium impact BCS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which include security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.
	Verify the Responsible Entity has reinforced security awareness at least once each calendar quarter.
	Verify the security awareness reinforcement included: • reinforcement of cyber security practices, or • reinforcement of physical security practices associated with cyber security.
	Verify that security awareness was reinforced for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to Applicable Systems.

Note to Auditor:

The Responsible Entity is not required to document that each quarter's reinforcement was received by each of its authorized personnel. Rather, the Responsible Entity is required to demonstrate that the security awareness reinforcement was communicated to its authorized personnel as a whole, not necessarily individually.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-8 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

R2 Part 2.1

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS with External Routable Connectivity (ERC) and their associated: 1. EACMS; and 2. PACS Medium impact BCS with Interactive Remote Access (IRA) SCI supporting an Applicable System in this Part	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information (BCSI) and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BCS; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including Transient Cyber Assets (TCA), and with Removable Media.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify that the training program(s) collectively include content on the following: 1. Cyber security policies; 2. Physical access controls; 3. Electronic access controls; 4. The visitor control program; 5. Handling of BCSI and its storage; 6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 7. Recovery plans for BCS; 8. Response to Cyber Security Incidents; and 9. Cyber security risks associated with a BCS electronic interconnectivity and interoperability with other Cyber Systems, including TCA, and with Removable Media.
	Verify the Responsible Entity's training program's content is appropriate to individual roles, functions, or responsibilities.
Notes to Auditor: 1. The training program(s) must collectively include all nine training elements. 2. It is not necessary that all nine training elements be included for the training of each role, function, or responsibility. 3. Each role, function, or responsibility must receive training on all appropriate training elements.	

Auditor Notes:

R2 Part 2.2

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R2, Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify all personnel completed the training specified in Part 2.1 prior to being granted authorized electronic access and authorized unescorted physical access to Applicable Systems, except during CIP Exceptional Circumstances.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

R2 Part 2.3

CIP-004-8 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Require completion of the training specified in Part 2.1 at least once every 15 calendar months (except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated individual training records.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify all personnel with authorized electronic access or authorized unescorted physical access to applicable Cyber Assets completed the training specified in Part 2.1 at least once every 15 calendar months, (except for medium impact BCS without ERC).

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

R3 Part 3.1

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that include a process to confirm identity.
	Verify a process to confirm identity was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

Auditor Notes:

R3 Part 3.2

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	Applicable Systems	Requirements	Measures
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1 current residence, regardless of duration; and 3.2.2 other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that include a process to perform a seven year criminal history records check that includes: 1. current residence, regardless of duration; 2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more; and 3. performing as much of the seven year criminal history records check as possible, if it is not possible to perform a full seven year criminal history records check.
	Verify a process to perform a seven year criminal history records check was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems and: • A full seven year criminal history records check was completed; or • The Responsible Entity completed as much of the seven year criminal history records check as possible, and documented the reason the full seven year criminal history records check was not completed.

Auditor Notes:

R3 Part 3.3

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process to evaluate criminal history records checks.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R3, Part 3.3

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that include criteria or a process to evaluate criminal history records checks for authorizing access.
	Verify the applicable criteria or process to evaluate criminal history records checks for authorizing access was implemented for personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems.

Auditor Notes:

R3 Part 3.4

CIP-004-8 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with IRA SCI supporting an Applicable System in this Part	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R3, Part 3.4

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that include criteria or a process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.
	Verify the criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3 was implemented.

Auditor Notes:

R3 Part 3.5

CIP-004-86 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with IRA SCI supporting an Applicable System in this Part	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.	Examples of evidence may include, but are not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R3, Part 3.5

This section to be completed by the Compliance Enforcement Authority

☐	Verify that the Responsible Entity has documented one or more personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to Applicable Systems that include a process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed, except during CIP Exceptional Circumstances, according to Parts 3.1 through 3.4 within the last seven years.
☐	For personnel with authorized electronic access and/or authorized unescorted physical access to Applicable Systems, verify the applicable personnel risk assessment process was implemented at least once every seven years.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations]*.

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-8 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

R4 Part 4.1

CIP-004-8 Table R4 – Access Management Program			
Part	Applicable Systems	Requirements	Measures
4.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1 Electronic access; 4.1.2 Unescorted physical access into a Physical Security Perimeter (PSP)(except for medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, dated documentation of the process to authorize electronic access, and unescorted physical access in a PSP.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R4, Part 4.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs which include a process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 1. Electronic access; and 2. unescorted physical access into a PSP
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
	Verify access was authorized, based on need, for: 1. Electronic access; and 2. unescorted physical access into a PSP
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

R4 Part 4.2

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-004-8, R4, Part 4.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs which include a process to verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.
	Verify the Responsible Entity has verified at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.

Auditor Notes:

R4 Part 4.3

CIP-004-8 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	Examples of evidence may include, but are not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R4, Part 4.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access management programs that, for electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.
	Verify the Responsible Entity has verified, at least once every 15 calendar months, that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-8 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R5 Part 5.1

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	A process to initiate removal of an individual's ability for unescorted physical access (except for Medium impact BCS without ERC) and Interactive Remote Access (IRA) upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-004-8, R5, Part 5.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs that include a process to initiate removal of an individual's ability for unescorted physical access and IRA upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).
	Verify the Responsible Entity has: 1. initiated removal of an individual's ability for unescorted physical access and IRA upon a termination action; and 2. completed the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).

Note to Auditor:

Removal of the ability for access does not necessarily require removal or disabling of the individual's accounts. The ability for access may be removed by disabling the individual's network access, confiscation of a badge, or other suitable means. Removal of IRA may be accomplished, for example, by disabling the individual's multi-factor authentication.

Auditor Notes:

R5 Part 5.2

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts; and authorized unescorted physical access (except for Medium impact BCS without ERC) that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	Examples of evidence may include, but are not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R5, Part 5.2

This section to be completed by the Compliance Enforcement Authority

☐	Verify the Responsible Entity has documented one or more access revocation programs for reassignments or transfers to revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.
☐	Verify the Responsible Entity has, for reassignments or transfers, revoked the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.
Note to Auditor: Revocation of access does not necessarily require removal of the individual's accounts. The account may be disabled in lieu of removal.	

Auditor Notes:

R5 Part 5.3

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	Examples of evidence may include, but are not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing revocation of access and dated within thirty calendar days of the termination actions.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R5, Part 5.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for termination actions to revoke the individual's non-shared user accounts (unless already revoked according to Requirement R5, Part 5.1), within 30 calendar days of the effective date of the termination action.
	Verify the Responsible Entity has, for termination actions, revoked the individual's non-shared user accounts (unless already revoked according to Requirement R5.1), within 30 calendar days of the effective date of the termination action.
Notes to Auditor: 1. If the access was already revoked under the actions taken for Requirement R5, Part 5.1, no further action is needed. 2. Revocation of access does not necessarily require removal or disabling of the individual's accounts. The ability for access may be removed by disabling the individual's network access, confiscation of a badge, or other suitable means. 3. Removal of Interactive Remote Access may be accomplished, for example, by disabling the individual's multi-factor authentication.	

Auditor Notes:

R5 Part 5.4

CIP-004-8 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination action. • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R5, Part 5.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more access revocation programs for termination actions to change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. The documented process(es) may include provisions for the Responsible Entity to determine and document that extenuating operating circumstances require a longer time period, and may change the password(s) within 10 calendar days following the end of the operating circumstances.
	If extenuating operating circumstances are invoked, verify the circumstances are documented and include a specific end date.
	For termination actions that do not invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 30 calendar days of the termination action.
	For termination actions that invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 10 calendar days following the end of the extenuating operating circumstances.
	For reassignments or transfers that do not invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 30 calendar days of the date that the Responsible Entity determines the individual no longer requires retention of the access.
	For reassignments or transfers that invoke extenuating operating circumstances, verify the passwords to shared accounts known to the user have been changed within 10 calendar days following the end of the extenuating operating circumstances.

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the Applicable Systems identified in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* that collectively include each of the applicable requirement parts in *CIP-004- 8 Table R6 – Access Management for BES Cyber System Information*. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys). *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning]*.

M6. Evidence must include each of the applicable documented programs that collectively include the applicable requirement parts in *CIP-004-8 Table R6 – Access Management for BES Cyber System Information* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R6 Part 6.1

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI (except for BCSI at a medium impact BCS without ERC).	Examples of evidence may include, but are not limited to, individual records or lists that include who is authorized, the date of the authorization, and the justification of business need for the provisioned access.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R6, Part 6.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more BCSI access management programs that include a process to, prior to provisioning, authorize (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 1. Provisioned electronic access to electronic BCSI; and 2. Provisioned physical access to physical BCSI.
	If the Responsible Entity has declared and responded to CIP Exceptional Circumstances, verify the Responsible Entity has adhered to the applicable cyber security policies.
	Verify the Responsible Entity has, prior to provisioning, authorized (unless already authorized according to Part 4.1) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 1. Provisioned electronic access to electronic BCSI; and 2. Provisioned physical access to physical BCSI.

Auditor Notes:

R6 Part 6.2

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium impact BCS with IRA SCI supporting an Applicable System in this Part	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	Examples of evidence may include, but are not limited to, the documentation of the review that includes all of the following: • List of authorized individuals; • List of individuals who have been provisioned access; • Verification that provisioned access is appropriate based on need; and • Documented reconciliation actions, if any.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R6, Part 6.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more BCSI access management programs that include a process to verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.
	Verify the Responsible Entity has verified at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.

Auditor Notes:

R6 Part 6.3

CIP-004-8 Table R6 – Access Management for BES Cyber System Information			
Part	**Applicable Systems**	**Requirements**	**Measures**
6.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PACS Medium Impact BCS with IRA SCI supporting an Applicable System in this Part	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) (except for BCSI at a Medium impact BCS without ERC) by the end of the next calendar day following the effective date of the termination action.	Examples of evidence may include, but are not limited to, access revocation records associated with the terminations and dated within the next calendar day of the termination action.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-004-8, R6, Part 6.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has, for termination actions, documented one or more BCSI access management programs that include a process to remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.
	Verify the Responsible Entity has, for termination actions, removed the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-004-8 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFT1v0	02/28/2024		Initial Draft

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-005-8 – Cyber Security – Electronic Security Perimeter(s)

This section to be completed by the Compliance Enforcement Authority.

Audit ID: Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity: Name of Registered Entity being audited
NCR Number: NCRnnnnn
Compliance Enforcement Authority: Region or NERC performing audit
Compliance Assessment Date(s)[2]: Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method: [On-site Audit | Off-site Audit | Spot Check]
Names of Auditors: Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		
R3	X	*	X	X		X			X	X		

*CIP-005-8 is only applicable to DPs that own certain UFLS, UVLS, RAS, protection systems, or cranking paths. See CIP-005-8 Section 4, Applicability, for details.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

---

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest version of the Reliability Standards, approved by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-8 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP.	Examples of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Systems connected via a routable protocol within each ESP.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

☐	Verify the Responsible Entity has documented one or more process(es) which require applicable Cyber Systems connected to a network via a routable protocol to be protected by a defined ESP.
☐	Verify each Cyber Asset of an Applicable System that is connected to a network via a routable protocol resides within a defined ESP.
☐	For each defined ESP, verify the identification of any associated PCA.

Notes to Auditor:

1. This Part is applicable to all high and medium impact BES Cyber Systems and their associated PCA regardless of External Routable Connectivity.
2. Those Cyber Assets that are part of a high or medium impact BES Cyber System that are not connected to a network via a routable protocol need not reside within a defined ESP.
3. For Cyber Assets that are part of a high or medium impact BES Cyber System that do not reside within a defined ESP, the absence of a connection to a network via a routable protocol will be verified.
4. The reason to identify an ESP without External Routable Connectivity is to identify the PCA associated with the ESP.
5. In order to verify that each Cyber Asset residing within a defined ESP has been identified as either a BES Cyber Asset or as a PCA, it may be necessary to examine the ESP and conduct an inventory of network connections within the ESP.
6. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same defined ESP.

Auditor Notes:

R1 Part 1.2

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS with ERC and their associated PCA Medium impact BCS with ERC and their associated PCA	Permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of system and documented reason, such as: • Electronic Access Point (EAP) configuration; • Network infrastructure configuration (e.g., technical policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); or • SCI configuration or settings (e.g., technical policies, hypervisor, fabric, back-plane, or SAN configuration).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which permit only needed routable protocol communications, documenting the reason, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.
	Verify that all External Routable Connectivity is through an identified EAP.
	For each defined ESP without an identified EAP, verify that no External Routable Connectivity exists.

Auditor Notes:

____

R1 Part 1.3

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting an Applicable System from Part 1.1 EACMS and their supporting SCI, that control an ESP for an Applicable System in Part 1.1	Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.	Examples of evidence may include, but are not limited to, documentation of the methods implemented to permit only needed network accessability to Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the Management Interfaces (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which Protect ESP and SCI configurations by implementing methods to permit only needed network accessibility to Management Interfaces of Applicable Systems, per system capability.
	For each Applicable System, verify only needed network accessibility to Management Interfaces of Applicable Systems, per system capability are permitted.

Auditor Notes:

R1 Part 1.4

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated PCA Medium impact BCS Band their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.4

This section to be completed by the Compliance Enforcement Authority

☐	Verify the Responsible Entity has documented one or more processes to perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, per system capability.
☐	For each Cyber Asset of an Applicable System, verify authentication is performed when establishing a dial-up connection, or that the system is incapable of authentication.

Note to Auditor:

If the Responsible Entity does not have or does not allow Dial-up Connectivity, the Responsible Entity is not required to document one or more processes to perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets. It is sufficient to verify that the Responsible Entity does not have Dial-up Connectivity.

Auditor Notes:

R1 Part 1.5

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious routable protocol communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.5

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which include one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.
	For each Applicable System, verify the Responsible Entity has implemented one or more methods for detecting known or suspected malicious routable protocol communications entering or leaving an ESP.

Auditor Notes:

____

R1 Part 1.6

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High impact BCS and their associated PCA Medium impact BCS at Control Centers and their associated PCA	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and i. ii. Time-sensitive communication of Protection Systems.	Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as: • Configurations or settings used to enforce encryption; or • The physical access restrictions (e.g.; cabling and components secured through conduit or secured cable trays).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R1, Part 1.6

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which include one or more methods for protecting the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time-sensitive communication of Protection Systems.
	For each Applicable System, verify the Responsible Entity has implemented one or more methods for protecting the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time-sensitive communication of Protection Systems.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in *CIP-005-8 Table R2 –Remote Access Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Permit Interactive Report Access (IRA), if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which permit IRA, if any, only through an Intermediate System.
	Verify all IRA utilizes an Intermediate System, or that the system is incapable of utilizing an Intermediate System.
	Verify that the Cyber Asset initiating IRA does not directly access an applicable Cyber Asset, or that or that the system is incapable of not directly accessing an applicable Cyber Asset.
	If a system is incapable of utilizing an Intermediate System or of not directly accessing an applicable Cyber Asset, verify that compensating measures are implemented.

Auditor Notes:

____

R2 Part 2.2

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	Intermediate System(s) used to access an Applicable System in Part 2.1	Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Examples of evidence may include, but are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption) initiate and terminate.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.
	Verify the Responsible Entity has documented one or more processes which Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.

Auditor Notes:

R2 Part 2.3

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	Intermediate System(s) used to access an Applicable System in Part 2.1	Require multi-factor authentication to the Intermediate System for IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Example of evidence may include, but are not limited to, architecture documents, configuration or settings detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which require multi-factor authentication to the Intermediate System for IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.
	Verify all IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System require multi-factor authentication, or that the system is incapable of requiring multi-factor authentication.
	If a system is incapable of requiring multi-factor authentication, verify that compensating measures are implemented.

Auditor Notes:

R2 Part 2.4

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including IRA and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which have one or more methods for determining active vendor remote access sessions (including IRA and system-to-system remote access).
	Verify all active vendor remote access sessions (including IRA and system-to-system remote access) can be determined, per system capability.
	If a system is incapable of determining all active vendor remote access sessions, verify that compensating measures are implemented.

Auditor Notes:

R2 Part 2.5

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access • (including IRA and system-to-system remote access).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.5

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which have one or more methods for disabling active vendor remote access sessions (including IRA and system-to-system remote access).
	Verify all active vendor remote access sessions (including IRA and system-to-system remote access) can be disabled
	If a system is incapable of disabling all active vendor remote access sessions, verify that compensating measures are implemented.

Auditor Notes:

R2 Part 2.6

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Intermediate System(s) used to access an Applicable System in Part 2.1	Prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System and supporting Cyber Systems.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.6

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.
	Verify the Responsible Entity implemented one or more processes to prevent Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs.
	If a system is incapable of preventing an Intermediate System(s) from sharing CPU resources and memory resources with any part of a high or medium impact BCS or associated PCAs, verify that compensating measures are implemented.

Auditor Notes:

R2 Part 2.7

CIP-005-8 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.7	Intermediate System(s) used to access an Applicable System in Part 2.1	Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.	Examples of evidence may include, but are not limited to, documentation that includes the following: • Network diagrams of Intermediate Systems architecture; or • Configuration, settings, or policy of the EAP which controls routable protocol communications of IRA through the ESP.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R2, Part 2.7

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to include routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.
	Verify the Responsible Entity implemented one or more processes to include Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP.
	If a system is incapable of including Routable protocol communications from an Intermediate System to a high or medium impact BCS or associated PCAs must be through an ESP, verify that compensating measures are implemented.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M3. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R3 Part 3.1

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS, PACS, and SCI			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part.	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	Examples of evidence may include, but are not limited to, documentation of the methods used to determine authenticated vendor-initiated remote connections, such as: • Methods for accessing logged or monitoring information to determine authenticated vendor-initiated remote connections.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-005-8 R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

☐	Verify the Responsible Entity has documented one or more processes which have one or more methods to determine authenticated vendor-initiated remote connections.
☐	Verify the Responsible Entity implemented one or more methods to determine authenticated vendor-initiated remote connections by implementing the documented process:

Note to Auditor:

When implementing the documented process, it should be either:

- Continuously, providing connection information in real time. In this case evidence of the continuous monitoring should be reviewed to verify the capability.
- On demand, initiated as needed by the Responsible Entity. In this case, a live demonstration or other means of verification of the ability may be used.

Auditor Notes:

R3 Part 3.2

CIP-005-8 Table R3 – Vendor Remote Access Management for EACMS and PACS			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	EACMS and PACS associated with high impact BCS. EACMS and PACS associated with medium impact BCS with ERC. SCI supporting an Applicable System in this Part.	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to terminate authenticated vendor-initiated remote connections to applicable systems. Examples include terminating an active vendor-initiated shell/process/session or dropping an active vendor-initiated connection in a firewall. Methods to control the ability to reconnect, if necessary, could be: disabling an Active Directory account; disabling a security token; restricting IP addresses from vendor sources in a firewall; or physically disconnecting a network cable to prevent a reconnection.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-005-8 R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes which have one or more methods to terminate authenticated vendor-initiated remote connections.
	Verify the Responsible Entity has documented one or more processes which have one or more methods to control the ability to reconnect authenticated vendor-initiated remote connections.
	Verify the Responsible Entity has implemented one or more methods for terminating authenticated vendor-initiated remote connections by implementing the documented process.
	Verify the Responsible Entity has implemented one or more methods for controlling the ability to reconnect authenticated vendor-initiated remote connections by implementing the documented process.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-005-8 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

Revision History for RSAW

Version	Date	Reviewers	Revision Description
V1	02/28/2024		Initial Draft

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-006-7 – Cyber Security — Physical Security of BES Cyber Systems

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X		X			X	X		
R2	X	X	X	X		X			X	X		
R3	X	X	X	X		X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

---

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-7 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

R1 Part 1.1

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium impact BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more physical security plans that define operational or procedural controls to restrict physical access.
	Verify the Responsible Entity has implemented the defined operational or procedural controls to restrict physical access to Applicable Systems.

Auditor Notes:

R1 Part 1.2

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium impact BCS with ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more physical security plans that utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access.
	Verify that each PSP has at least one physical access control.
	Verify that only those individuals with authorized unescorted physical access are allowed unescorted physical access into each applicable PSP.

Auditor Notes:

____

R1 Part 1.3

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access, per system capability.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more physical security plans that utilize two or more different physical access controls (this does not require two completely independent PACS) to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access, per system capability.
	Verify that each PSP has at least two physical access controls per system capability.

	Verify that only those individuals with authorized unescorted physical access are allowed authorized unescorted physical access into each applicable PSP.
	If a system is not capable of utilizing two or more different physical access controls, verify the incapabilities of the system.

Auditor Notes:

R1 Part 1.4

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting Applicable Systems in this Part	Monitor for unauthorized access through a physical access point into a PSP.	Examples of evidence may include, but are not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a PSP.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R1, Part 1.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more physical security plans to monitor for unauthorized access through a physical access point into a PSP.
	Verify that the Responsible Entity monitors for unauthorized access through a physical access point into

☐	a PSP.

Auditor Notes:

R1 Part 1.5

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a PSP and additional evidence that the alarm or alert was issued and communicated as identified in the Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R1, Part 1.5

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more physical security plans to issue an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to the

	personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.
	Verify that an alarm or alert is issued in response to detected unauthorized access through a physical access point into a PSP to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.

Auditor Notes:

R1 Part 1.6

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Monitor each PACS for unauthorized physical access to a PACS.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R1, Part 1.6

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more physical security plans to monitor each PACS for unauthorized physical access to a PACS.
	Verify that each PACS is monitored for unauthorized physical access to a PACS.

Auditor Notes:

R1 Part 1.7

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	PACS associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Issue an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to PACS and additional evidence that the alarm or alerts was issued and communicated as identified in the Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R1, Part 1.7

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more physical security plans to issue an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the Cyber Security Incident response plan within 15 minutes of the detection.

☐	Verify that an alarm or alert is issued in response to detected unauthorized physical access to a PACS to the personnel identified in the Cyber Security Incident response plan within 15 minutes of detection.

Auditor Notes:

R1 Part 1.8

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each PSP, with information to identify the individual and date and time of entry.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes logging and recording of physical entry into each PSP and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into each PSP that show the individual and the date and time of entry into each PSP.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R1, Part 1.8

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more physical security plans to log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each PSP, with information to identify the individual and date and time

	of entry.
	Verify that logs of entry of each individual with authorized unescorted physical access into each PSP, contains information to identify the individual and date and time of entry.

Auditor Notes:

R1 Part 1.9

CIP-006-7 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into each PSP that show the date and time of entry into each PSP.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R1, Part 1.9

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more physical security plans to retain physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days.

☐	Verify that physical access logs of entry of individuals with authorized unescorted physical access into each PSP are retained for at least 90 calendar days.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented visitor control program(s) that include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each PSP.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as visitor logs.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more visitor control programs to require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each PSP.
	Verify that the Responsible Entity has implemented a program for continuous escort of individuals who are provided access but are not authorized for unescorted physical access within each PSP.
	If the Responsible Entity has experienced an exception for CIP Exceptional Circumstances, verify the Responsible Entity has adhered to any applicable cyber security policies.

Auditor Notes:

R2 Part 2.2

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Require manual or automated logging of visitor entry into and exit from each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor.	Examples of evidence may include, but are not limited to, language in a visitor control program that requires continuous escorted access of visitors within each PSP and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R2, Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more visitor control programs to require manual or automated logging of visitor entry into and exit from each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible

	for the visitor.
	Verify that the Responsible Entity performs manual or automated logging of visitor entry into and exit from each PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor.
	If the Responsible Entity has experienced an exception for CIP Exceptional Circumstances, verify the Responsible Entity has adhered to any applicable cyber security policies.

Auditor Notes:

R2 Part 2.3

CIP-006-7 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated: 1. EACMS; and 2. PCA Medium impact BCS with ERC and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Retain visitor logs for at least 90 calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least 90 calendar days.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-006-7, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more visitor control programs to retain visitor logs for at least 90 calendar days.
	Verify that visitor logs are retained for at least 90 calendar days.

☐	If the Responsible Entity has experienced an exception for CIP Exceptional Circumstances, verify the Responsible Entity has adhered to any applicable cyber security policies.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-7 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R3 Part 3.1

CIP-006-7 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	PACS associated with: • High impact BCS, or • Medium impact BCS with ERC Locally mounted hardware or devices at the PSP associated with: • High impact BCS, or • Medium impact BCS with ERC	Maintenance and testing of each PACS and locally mounted hardware or devices at each PSP at least once every 24 calendar months to ensure they function properly.	Examples of evidence may include, but are not limited to, a maintenance and testing program that provides for testing each PACS and locally mounted hardware or devices associated with each applicable PSP at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-006-7, R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more PACS maintenance and testing programs for maintenance and testing of each PACS and locally mounted hardware or devices at each PSP at least once every 24 calendar months to ensure they function properly.
	Verify that maintenance and testing of each PACS and locally mounted hardware or devices at each PSP is conducted at least once every 24 calendar months to ensure they function properly.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-006-7 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFT1v0	02/28/2024		Initial Draft

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-007-7 — Cyber Security – System Security Management

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X		X			X	X		
R2	X	X	X	X		X			X	X		
R3	X	X	X	X		X			X	X		
R4	X	X	X	X		X			X	X		
R5	X	X	X	X		X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

---

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			
R4			
R5			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R1 – System Hardening* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-007-7 Table R1– System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports or network accessible logical services, individually or by group; • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; or • Configuration or settings of host-based firewalls or other device level mechanisms that disable or prevent unneeded network accessable logical ports or network accessible logical services; or • Identity or process based access policy or workload configuration demonstrating needed network accessibility.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-007-7, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.
	Verify the Responsible Entity has implemented one or more processes to disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.
	If a system is incapable of disabling or preventing unnedded routable protocol network accessibility on each Applicable System, verify that compensating measures are implemented.

Auditor Notes:

R1 Part 1.2

CIP-007-7 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. Medium impact BCS at Control Centers and their associated: 1. PCA; and 2. Nonprogrammable communication components located inside both a PSP and an ESP. SCI supporting an Applicable System in this Part.	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Examples of evidence may include, but are not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes that protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.
	For each Cyber Asset of an Applicable System, verify that the unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media are protected against use.

Auditor Notes:

R1 Part 1.3

CIP-007-7 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI supporting either: High impact BCS and their associated PCA. Medium impact BCS and their associated PCA.	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as: • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes that mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.
	Verify the Responsible Entity has implemented one or more processes that mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU resources and memory resources, excluding storage resources, between VCAs that are, or are associated with, a medium or high impact BCS, and VCAs that are not, or are not associated with, a medium or high impact BCS.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Cyber Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R2 – Cyber Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.	Examples of evidence may include, but are not limited to, documentation of a patch management process and documentation or lists of sources that are monitored.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-007-7, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more patch management processes for tracking, evaluating, and installing cyber security patches for Applicable Systems.
	Verify that the tracking portion of each patch management process includes the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.
	For each Applicable System, verify at least one of the following is true: • The Responsible Entity has identified one or more patching sources; • The Responsible Entity has documented that the Applicable System is not updateable; or • The Responsible Entity has documented that no patching source exists.

Auditor Notes:

R2 Part 2.2

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Examples of evidence may include, but are not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of cyber security patches released by the documented sources at least once every 35 calendar days.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R2, Part 2.2

This section to be completed by the Compliance Enforcement Authority

☐	Verify the Responsible Entity has documented one or more processes to evaluate cyber security patches

	for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1, at least once every 35 calendar days.
	For each identified patch source, verify that cyber security patches have been evaluated for applicability at least once every 35 calendar days.
	For each identified patch source, verify the results of the evaluations for applicability.

Auditor Notes:

R2 Part 2.3

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BES Cyber System and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the cyber security patch (e.g., exports from automated patch management tools that provide installation date, verification of component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the cyber security patch and a timeframe for the completion of these mitigations.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes, for applicable patches identified in Part 2.2, to take one of the following actions within 35 calendar days of the evaluation completion: • Apply the applicable patches; • Create a dated mitigation plan; or • Revise an existing mitigation plan.
	Verify the Responsible Entity has documented one or more processes for its mitigation plans that requires the inclusion of planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.
	For each applicable cyber security patch, verify that one of the following actions was taken within 35 calendar days of the completion of the evaluation for applicability: • The patch was applied to all devices for which it is applicable; • A mitigation plan was created; or • A mitigation plan was revised.
	In the case where a mitigation plan was created or revised, verify the mitigation plan includes planned actions to mitigate the vulnerabilities addressed by each cyber security patch, and that the mitigation plan includes a timeframe for completion.
Note to Auditor: Entities may choose to use a single mitigation plan for multiple patches. In this case, the mitigation plan must have planned actions to mitigate the vulnerabilities addressed by each security patch.	

Auditor Notes:

R2 Part 2.4

CIP-007-7 Table R2 – Cyber Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Examples of evidence may include, but are not limited to, records of implementation of mitigations, and any approval records for mitigation plan revisions or extensions.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R2, Part 2.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes that, for each mitigation plan

	created or revised in Part 2.3, require implementation of the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.
	For each completed mitigation plan: 1. Verify the mitigation plan was completed by implementing all provisions of the mitigation plan; 2. Verify the mitigation plan was completed within the specified timeframe; and 3. If a revision or an extension was made to a mitigation plan, verify the revision or extension was approved by the CIP Senior Manager or delegate.
	For each active mitigation plan: 1. Verify the mitigation plan has not exceeded its implementation timeframe, or its approved extension, if any. 2. If a revision or an extension was made to a mitigation plan, verify the revision or extension was approved by the CIP Senior Manager or delegate.

Auditor Notes:

____

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations]*.

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R3 Part 3.1

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Deploy method(s) to deter, detect, or prevent malicious code.	Examples of evidence may include, but are not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to deploy method(s) to deter, detect, or prevent malicious code.
	Verify that each Applicable System has one or more documented methods deployed to deter, detect, or prevent malicious code.

Auditor Notes:

R3 Part 3.2

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes that mitigate the threat of

☐	detected malicious code.
☐	For each instance of detected malicious code, verify the threat of the malicious code was mitigated.

Note to Auditor:

It may not be necessary to remove malicious code from a device in order to mitigate the threat of that malicious code. For example, it may be possible to contain malicious code by blocking communication with its command and control servers and by preventing its spread to other systems. Then the malicious code can be removed at a later time such as a plant outage.

Auditor Notes:

R3 Part 3.3

CIP-007-7 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Examples of evidence may include, but are not limited to, documentation showing the process used for the update of signatures or patterns.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R3, Part 3.3

This section to be completed by the Compliance Enforcement Authority

	For those methods identified in Part 3.1 that use signatures or patterns, verify the Responsible Entity

	has documented one or more processes to update the signatures or patterns. The process must address testing and installing the signatures or patterns.
	For each method deployed to deter, detect, or prevent malicious code that uses signatures or patterns, verify the associated process addresses testing and installing updates to signatures or patterns.
	For each method deployed to deter, detect, or prevent malicious code that uses signatures or patterns, verify the associated process is implemented.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-7 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in CIP-007-7 Table R4 – Security Event Monitoring and additional evidence to demonstrate implementation as described in the Measures column of the table.

R4 Part 4.1

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Log security events per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the Applicable System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R4, Part 4.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 1. Detected successful login attempts; 2. detected failed access attempts and failed login attempts; and 3. detected malicious code.
	For each event type required for identification of or after the fact investigation of Cyber Security Incidents: • If logging of the event type is performed at the BES Cyber System level, for each Applicable System, verify: ○ The BES Cyber System is capable of, and configured for, logging the event type; ○ The BES Cyber System is generating logs of the event type; or ○ The BES Cyber System is not capable of logging the event type. • If logging of the event type is performed at the Cyber Asset level, for each Cyber Asset of an Applicable System, verify: ○ The Cyber Asset is capable of, and configured for, logging the event type; ○ The Cyber Asset is generating logs of the event type; or ○ The Cyber Asset is not capable of logging the event type.

Auditor Notes:

R4 Part 4.2

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events, per system capability: 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R4, Part 4.2

This section to be completed by the Compliance Enforcement Authority

☐	Verify the Responsible Entity has documented one or more processes to generate alerts for security

	events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events per system capability: 1. Detected malicious code from Part 4.1; and 2. detected failure of Part 4.1 event logging.
	Verify the Responsible Entity has determined the security events that necessitate an alert.
	Verify the security events determined to necessitate an alert include, at a minimum: 1. Detected malicious code; and 2. detected failure of logging.
	For each of the security events determined to necessitate an alert: 1. If alerting is performed on a per Cyber Asset basis, is the Cyber Asset capable of alerting on the event type? 1. If yes, verify either: i. Alerting is configured for the Cyber Asset for the event type; or ii. an actual alert has been generated. 2. If no, verify the inability of the Cyber Asset to generate an alert for the event type. 2. If alerting is performed on a per BES Cyber System basis, is the BES Cyber System capable of alerting on the event type? 1. If yes, verify either: i. Alerting is configured for the BES Cyber System for the event type; or ii. an actual alert has been generated. 2. If no, verify the inability of the BES Cyber System to generate an alert for the event type.

Auditor Notes:

R4 Part 4.3

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Retain applicable security event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 calendar days or greater.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R4, Part 4.3

This section to be completed by the Compliance Enforcement Authority

☐	Verify the Responsible Entity has documented one or more processes to retain applicable security event

	logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.
	For each Applicable System, verify logs are retained for at least 90 consecutive calendar days unless: • The system is incapable of retaining logs; or • A documented CIP Exceptional Circumstance exists.
	If a system is incapable of retaining logs for at least 90 consecutive calendar days, verify that compensating measures are implemented.
	If the Responsible Entity has experienced an exception for CIP Exceptional Circumstances, verify the Responsible Entity has adhered to any applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

R4 Part 4.4

CIP-007-7 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, findings from the review (if any), and dated documentation showing the review occurred.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R4, Part 4.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.
	Verify the Responsible Entity reviews a summary or sampling of logged security events at least every 15 calendar days to identify otherwise undetected Cyber Security Incidents.

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-7 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-7 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R5 Part 5.1

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Have a method(s) to enforce authentication of interactive user access, per system capability.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to have a method(s) to enforce authentication of interactive user access, per system capability.
	For each Applicable System, verify the Responsible Entity enforces authentication of interactive user access per system capability
	If a system is incapable of enforcing authentication of interactive user access, verify that compensating measures are implemented.

Auditor Notes:

R5 Part 5.2

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Examples of evidence may include, but are not limited to, a listing of accounts by account types showing the enabled default or generic account types in use.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by

	location, or by system type(s).
	For each Cyber Asset of an Applicable System, verify the Responsible Entity has identified and inventoried all known enabled default or other generic account types. These account types may be identified by system, by groups of systems, by location, or by system type.

Auditor Notes:

R5 Part 5.3

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Identify individuals who have authorized access to shared accounts.	Examples of evidence may include, but are not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to identify individuals who have authorized access to shared accounts.

☐	For each Cyber Asset of an Applicable System, verify the Responsible Entity has identified individuals with authorized access to shared accounts.

Note to Auditor:
The Responsible Entity is permitted flexibility in the way shared accounts may be documented. Shared accounts may be documented by Cyber Asset or BES Cyber System. Additionally, individuals with authorized access to shared accounts may be listed individually or by role.

Auditor Notes:

R5 Part 5.4

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Change known default passwords, per system capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to change known default passwords, per system capability.

☐	For Applicable Systems with the capability to change default passwords, verify the Responsible Entity has changed the known default passwords.
☐	If a system is incapable of changing default passwords, verify that compensating measures are implemented.

Auditor Notes:

R5 Part 5.5

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.5

This section to be completed by the Compliance Enforcement Authority

	For password-only authentication for interactive user access, verify the Responsible Entity has documented one or more processes to either technically or procedurally enforce the following password parameters: 1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 2. minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Applicable System.
	For each Applicable System, for password-only authentication for interactive user access, verify password length is enforced by either technical or procedural methods, per 5.5.1.
	For each Applicable System, for password-only authentication for interactive user access, verify password complexity is enforced by either technical or procedural methods, per 5.5.2.
Note to Auditor: This Part does not apply to multi-factor authentication.	

Auditor Notes:

R5 Part 5.6

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Examples of evidence may include, but are not limited to: • System-generated reports or screenshots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.6

This section to be completed by the Compliance Enforcement Authority

	For password-only authentication for interactive user access, verify the Responsible Entity has documented one or more processes to either technically or procedurally enforce password changes or

	an obligation to change the password at least once every 15 calendar months, per system capability.
	For Applicable Systems, if a password for password-only authentication for interactive user access cannot be changed, verify that the system is incapable of changing the password.
	For Applicable Systems, if a password for password-only authentication for interactive user access can be changed, verify a password change, at least every 15 calendar months, is enforced by either technical or procedural methods.
	If a system is incapable of changing a password for password-only authentication for interactive user access, verify that compensating measures are implemented.
Note to Auditor: This Part does not apply to multi-factor authentication.	

Auditor Notes:

R5 Part 5.7

CIP-007-7 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration or settings showing how the system notified individuals after a determined number of unsuccessful login attempts.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-007-7, R5, Part 5.7

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes to either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication

	attempts, per system capability.
	If the number of unsuccessful authentication attempts is limited, verify the configuration.
	If alerts are generated after a threshold of unsuccessful authentication attempts, verify the evidence of configuration supports this method.
	If neither method is used, verify that compensating measures are implemented.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-007-7 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFTv1	02/28/2024		Initial Draft

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-008-7 – Cyber Security — Incident Reporting and Response Planning

This section to be completed by the Compliance Enforcement Authority.

Audit ID: Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity: Name of Registered Entity being audited
NCR Number: NCRnnnnn
Compliance Enforcement Authority: Region or NERC performing audit
Compliance Assessment Date(s)[2]: Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method: [On-site Audit | Off-site Audit | Spot Check]
Names of Auditors: Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		
R3	X	*	X	X		X			X	X		
R4	X	*	X	X		X			X	X		

*CIP-008-7 is only applicable to DPs that own certain UFLS, UVLS, RAS, protection systems, or cranking paths. See CIP-003-8 Section 4, Applicability, for details.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

---

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest version of the Reliability Standards, approved by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request from the registered entity additional evidence that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			
R4			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications*.

R1 Part 1.1

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated Electronic Access Control and Monitoring Systems (EACMS) Medium impact BCS and their associated EACMS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process(es) to identify, classify, and respond to Cyber Security Incidents.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-7, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which include one or more processes to identify, classify, and respond to Cyber Security Incidents.

Auditor Notes:

R1 Part 1.2

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	One or more processes: 1.2.1. That include criteria to evaluate and define attempts to compromise; 1.2.2. To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and 1.2.3. To provide notification per Requirement R4.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents or a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the "Applicable Systems" column including justification for attempt determination criteria and documented processes for notification.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-7, R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which include one or more processes that include criteria to evaluate and define attempts to compromise.
	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which include one or more processes to determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • an attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the “Applicable Systems” column for this Part.
	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which include one or more processes to provide notification per Requirement R4.
Note to Auditor: If the Responsible Entity is prohibited by law from reporting to the E-ISAC, then the process need not include a provision for reporting to the E-ISAC. If this provision is invoked, the audit team should verify that the Responsible Entity is prohibited by law from reporting to the E-ISAC. If the Responsible Entity is within U.S. jurisdiction, but is prohibited by law from reporting to the NCCIC, then the process need not include a provision for reporting to the NCCIC. If this provision is invoked, the audit team should verify that the Responsible Entity is prohibited by law from reporting to the NCCIC.	

Auditor Notes:

R1 Part 1.3

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-7, R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which define the roles and responsibilities of Cyber Security Incident response groups or individuals.

Auditor Notes:

R1 Part 1.4

CIP-008-7 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Incident handling procedures for Cyber Security Incidents.	Examples of evidence may include, but are not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-7, R1, Part 1.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more Cyber Security Incident response plans which include incident handling procedures for Cyber Security Incidents.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.*

R2 Part 2.1

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-008-7, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has tested each Cyber Security Incident response plan at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • with a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • with an operational exercise of a Reportable Cyber Security Incident.

Auditor Notes:

R2 Part 2.2

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident response or exercise.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-7 R2 Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity used the Cyber Security Incident response plan(s) reviewed under Requirement R1 when responding to a Reportable Cyber Security Incident, when responding to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or when performing an exercise of a Reportable Cyber Security Incident.
	Verify the Responsible Entity has documented deviations from the plan(s), if any, taken during the response to the Reportable Cyber Security Incident, to the Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or during the performance of an exercise of a Reportable Cyber Security Incident.

Note to Auditor:

The practice of incident response requires the ability to be flexible when responding to Cyber Security Incidents. This is acknowledged by this Part's provision for documenting deviations from the Responsible Entity's incident response plan. The auditor should note that, while deviations from the incident response plan are permissible, deviations from the language of the Requirement (testing of the plan at least once every 15 calendar months, notification to the E-ISAC and NCCIC of applicable incidents, etc.), are not permissible.

Auditor Notes:

R2 Part 2.3

CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the “Applicable Systems” column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	Examples of evidence may include, but are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-7, R2, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has retained records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.*

R3 Part 3.1

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.2.1. Document any lessons learned or document the absence of any lessons learned; 3.2.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.1. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-7, R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify that no later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response, the Responsible Entity has: 1. Documented any lessons learned or documented the absence of any lessons learned; 2. updated the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3. notified each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.

Auditor Notes:

____

R3 Part 3.2

CIP-008-7 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	Examples of evidence may include, but are not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or Training sign-in sheets.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-7, R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify that no later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan, the Responsible Entity has: 1. Updated the Cyber Security Incident response plan(s); and 2. notified each person or group with a defined role in the Cyber Security Incident response plan of the updates.

Auditor Notes:

____

R4 Supporting Evidence and Documentation

R4. Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States Cybersecurity & Infrastructure Security Agency (CISA), or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1 Part 1.2.1, a system identified in the Applicable Systems column, unless prohibited by law, in accordance with each of the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M4. Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise a system identified in the Applicable Systems column according to the applicable requirement parts in *CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents*.

R4 Part 4.1

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known: 4.1.1. The functional impact; 4.1.2. The attack vector used; and 4.1.3. The level of intrusion that was achieved or attempted.	Examples of evidence may include, but are not limited to, dated documentation of initial notifications and updates to the E-ISAC and CISA, or their successors.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-7, R4, Part 4.1

This section to be completed by the Compliance Enforcement Authority

	Verify the initial notifications and updates included, to the extent known at the time: 1. The functional impact; 2. The attack vector used; and 3. The level of intrusion that was achieved or attempted.

Auditor Notes:

R4 Part 4.2

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	Applicable Systems	Requirements	Measures
4.2	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the Applicable Systems column for this Part.	Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and CISA, or their successors.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-7, R4, Part 4.2

This section to be completed by the Compliance Enforcement Authority

	For each Reportable Cyber Security Incident as identified pursuant to the process(es) specified in Requirement R1, Part 1.2, verify that the initial notification was submitted to each applicable agency within one hour after the determination of a Reportable Cyber Security Incident.
	For each Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part, as identified pursuant to the process specified in Requirement R1, Part 1.2, verify that the initial notification was submitted to each applicable agency by the end of the next calendar day after a determination of a Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part.

Auditor Notes:

R4 Part 4.3

CIP-008-7 Table R4 – Notifications and Reporting for Cyber Security Incidents			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Provide updates, if any, within seven calendar days of determination of new or changed attribute information required in Part 4.1.	Examples of evidence may include, but are not limited to, dated documentation of submissions to the E-ISAC and CISA, or their successors.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-008-7, R4, Part 4.3

This section to be completed by the Compliance Enforcement Authority

	For each Reportable Cyber Security Incident and each Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column for this Part, verify updates, if any, were provided within seven calendar days of determination of new or changed attribute information.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-008-7 may be found on the NERC web site (www.nerc.com) under "Program Areas & Departments", "Standards", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC web site.

In addition to the Reliability Standard, there is background information available on the NERC web site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC web site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards because it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

Selected Glossary Terms

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Cyber Security Incident

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises, or attempts to compromise, (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or
- Disrupts, or attempts to disrupt, the operation of a BES Cyber system.

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BES Cyber System; or
- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFTv1	02/28/2024		Initial Draft

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-009-7 – Cyber Security – Recovery Plans for BES Cyber Systems

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X		X			X	X		
R2	X	X	X	X		X			X	X		
R3	X	X	X	X		X			X	X		
R4	X	X	X	X		X			X	X		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

---

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable Requirement Parts in *CIP-009-7 Table R1 – Recovery Plan Specifications*.

R1 Part 1.1

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems(EACMS); and 2. Physical Access Control Systems(PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-009-7, R1 Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more recovery plans which include conditions for activation of the recovery plan(s).

Auditor Notes:

R1 Part 1.2

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	Examples of evidence may include, but are not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-009-7, R1 Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more recovery plans which define roles and responsibilities of responders.

Auditor Notes:

R1 Part 1.3

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover Applicable System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover Applicable System functionality.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-009-7, R1 Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more recovery plans which include one or more processes for the backup and storage of information required to recover Applicable System functionality.

Auditor Notes:

R1 Part 1.4

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Examples of evidence may include, but are not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-009-7, R1 Part 1.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more recovery plans which include one or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.

Auditor Notes:

R1 Part 1.5

CIP-009-7 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	One or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Examples of evidence may include, but are not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-009-7, R1 Part 1.5

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more recovery plans which include one or more processes to preserve data, per system capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.

Auditor Notes:

____

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable Requirement Parts in *CIP-009-7 Table R2 – Recovery Plan Implementation and Testing.*

R2 Part 2.1

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	Examples of evidence may include, but are not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-009-7, R2 Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has tested each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • with a paper drill or tabletop exercise; or • with an operational exercise.

Auditor Notes:

R2 Part 2.2

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover Applicable System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover Applicable System functionality substitutes for this test.	Examples of evidence may include, but are not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-009-7, R2 Part 2.2

This section to be completed by the Compliance Enforcement Authority

	For each recovery plan, verify either: • The Responsible Entity has tested a representative sample of information used to recover Applicable System functionality at least once every 15 calendar months to ensure that the

	information is useable and is compatible with current configurations; or • the Responsible Entity has performed an actual recovery that incorporates the information used to recover Applicable System functionality.

Auditor Notes:

R2 Part 2.3

CIP-009-7 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High impact BCS	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-009-7, R2 Part 2.3

This section to be completed by the Compliance Enforcement Authority

	For each recovery plan, verify either: • The Responsible Entity has tested each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an

	environment representative of the production environment; or • the Responsible Entity has performed an actual recovery response.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable Requirement Parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the Applicable Requirement parts in *CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication.*

R3 Part 3.1

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-009-7, R3 Part 3.1

This section to be completed by the Compliance Enforcement Authority

	Verify that no later than 90 calendar days after completion of a recovery plan test or actual recovery, the Responsible Entity has: 1. Documented any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 2. updated the recovery plan based on any documented lessons learned associated with the plan; and 3. notified each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.

Auditor Notes:

R3 Part 3.2

CIP-009-7 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	Examples of evidence may include, but are not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-009-7, R3 Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify that no later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan, the Responsible Entity has: 1. Updated the recovery plan; and 2. notified each person or group with a defined role in the recovery plan of the updates.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-009-7 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFTv1	02/28/2024		Initial Draft

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-010-5 – Cyber Security – Configuration Change Management and Vulnerability Assessments

This section to be completed by the Compliance Enforcement Authority.

Audit ID: Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity: Name of Registered Entity being audited
NCR Number: NCRnnnnn
Compliance Enforcement Authority: Region or NERC performing audit
Compliance Assessment Date(s)[2]: Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method: [On-site Audit | Off-site Audit | Spot Check]
Names of Auditors: Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		
R3	X	*	X	X		X			X	X		
R4	X	*	X	X		X			X	X		

*CIP-010-5 is only applicable to DPs that own certain UFLS, UVLS, RAS, protection systems, or cranking paths. See CIP-010-5 Section 4, Applicability, for details.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

---

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest version of the Reliability Standards, approved by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request from the registered entity additional evidence that is not included in this RSAW. Additionally, this RSAW may include excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			
R4			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall implement one or more documented process(es) to manage configuration changes, individually or by group, that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1* – Configuration Change Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control or Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Accet (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.	Examples of evidence may include, but are not limited to, one or more documented process(es) that authorize changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity, such as: • Change records documenting the authorization. • Change records authorizing systems to automate changes to Applicable Systems. Examples of changes that may alter the behavior of one or more cyber security controls may include, but are not limited to: • Installation, removal, or update of operating system, firmware, software, or cyber security patches, including changes to VCA parent images from which Applicable Systems will be instantiated (CIP-007 R1.1, R2) • Configuration changes that affect routable protocol network accessibility (CIP-007 R1.1) • Configuration changes affecting the establishment of, or access control through, an ESP (CIP-005 R1, R2) • Configuration of malicious code prevention methods (CIP-007 R3) • Configuration of security event logging/alerting (CIP-007 R4) • Configuration changes to authentication methods (e.g., a password enforcement policy change, but not users changing their password) (CIP-007 R5) • Configuration changes to CPU/memory sharing of VCAs on SCI (CIP-007 R1.3)

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more processes that include the authorization of changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.
	Verify that the Responsible Entity has implemented one or more processes that include the authorization of changes that affect Applicable Systems where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-005 or CIP-007, as defined by the Responsible Entity.

Auditor Notes:

R1 Part 1.2

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS	1.2.1 Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test, or logs from systems that automatically remediate deviations in required cyber security controls in CIP-005 and CIP-007.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-010-5 R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more processes that include: 1.2.1 Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, to ensure that required cyber security controls in CIP-005 and CIP- 007 are not adversely affected; and 1.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.
	Verify that the Responsible Entity has implemented one or more processes that include: 1.2.1 Prior to implementing any change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, to ensure that required cyber security controls in CIP-005 and CIP- 007 are not adversely affected; and 1.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

Auditor Notes:

R1 Part 1.3

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part. Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to installation or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-010-5 R1, Part 1.3

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more processes that include: Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.
	Verify that the Responsible Entity has implemented one or more processes that include: Prior to the installation of operating systems, firmware, software, or software patches and when the method to do so is available to the Responsible Entity from the software source: 1.3.1. Verify the identity of the software source; and 1.3.2. Verify the integrity of the software obtained from the software source.

Auditor Notes:

R1 Part 1.4

CIP-010-5 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	As a part of the changes authorized per Part 1.1, verify that the behavior(s) of the altered cyber security controls were not adversely affected.	An example of evidence may include, but is not limited to: • System generated evidence of automated verification of required behaviors. • Records from a verification process showing that, as a part of the change process, the required behavior(s) of the altered security controls remain effective, were corrected, or the change was reversed.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R1, Part 1.4

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented one or more processes that include verification that the behavior(s) of the altered cyber security controls were not adversely affected as a part of the changes authorized per Part 1.1.
	Verify that the Responsible Entity has implemented one or more processes that include verification that the behavior(s) of the altered cyber security controls were not adversely affected as a part of the changes authorized per Part 1.1.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement one or more documented process(es) to monitor configuration changes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-010-5 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BES Cyber System and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Methods to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods; 2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, documented methods to monitor at least once every 35 calendar days. Monitoring system configuration or procedural controls demonstrating monitoring of at least one cyber security control for 2.1.1 through 2.1.7. Examples of evidence may include, but are not limited to, reports generated from automated tools or manual reviews along with records of investigation for any unauthorized changes that were detected. Note: monitoring of VCA parent images from which Applicable Systems will be instantiated is an example of an automated control for 2.1.3.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity documented one or more processes to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods; 2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.
	Verify the Responsible Entity implemented one or more processes to monitor, per system capability, at least once every 35 calendar days, for unauthorized changes that affect Applicable Systems, where those changes alter the behavior of one or more cyber security controls, excluding procedural and physical controls, serving one or more requirement parts in CIP-007, as defined by the Responsible Entity; that include at least one cyber security control for each of the following: 2.1.1. Configuration on each Applicable System that affects its routable protocol network accessibility; 2.1.2. Configuration of CPU or memory sharing of VCAs on SCI; 2.1.3. Installation, removal, and update of operating system, firmware, software, and cyber security patches. 2.1.4. Configuration of malicious code protection methods; 2.1.5. Configuration of security event logging or alerting; 2.1.6. Configuration of authentication methods; and 2.1.7. Changes to the enabled or disabled status of accounts. Document and investigate detected unauthorized changes.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-5 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R3 Part 3.1

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-010-5 R3, Part 3.1

This section to be completed by the Compliance Enforcement Authority

☐	Verify the Responsible Entity documented one or more processes for conducting a paper or active vulnerability assessment at least once every 15 calendar months.
☐	For each Applicable System, verify the Responsible Entity conducted a paper or active vulnerability assessment at least once every 15 calendar months.

Auditor Notes:

R3 Part 3.2

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High impact BES Cyber Systems. SCI supporting an Applicable System in this Part.	At least once every 36 calendar months, per system capability: 3.2.1 Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-010-5 R3, Part 3.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity documented one or more processes to: 1. Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 2. document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.
	Verify the Responsible Entity implemented one or more processes to: 1. Perform an active vulnerability assessment in a test environment that minimizes differences with the production environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects; and 2. document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.
	For each Applicable System, per system capability, verify an active vulnerability assessment was conducted at least once every 36 calendar months, in accordance with 3.2.1; and results of testing was documented, in accordance with 3.2.2.
	If a system is incapable of conducting an active vulnerability assessment at least once every 36 months, verify that compensating measures are implemented.

Auditor Notes:

R3 Part 3.3

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part.	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements or additions with a previously assessed configuration of an existing Applicable System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of tools used to perform the assessment; or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R3, Part 3.3

This section to be completed by the Compliance Enforcement Authority

☐	Verify the Responsible Entity documented one or more processes for performing an active vulnerability assessment on each new Applicable System, prior to it becoming a new Applicable System, except for CIP Exceptional Circumstances and like replacements of the same type with a baseline configuration that models an existing baseline configuration of the previous or other existing Applicable System.
☐	Verify the Responsible Entity implemented one or more processes for performing an active vulnerability assessment on each new Applicable System, prior to it becoming a new Applicable System, except for CIP Exceptional Circumstances and like replacements of the same type with a baseline configuration that models an existing baseline configuration of the previous or other existing Applicable System.
☐	If the Responsible Entity has experienced an exception for CIP Exceptional Circumstances, verify the Responsible Entity has adhered to any applicable cyber security policies.
Note to Auditor: The Responsible Entity may reference a separate set of documents to demonstrate its response to any requirements impacted by CIP Exceptional Circumstances.	

Auditor Notes:

____

R3 Part 3.4

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.4	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Examples of evidence may include, but are not limited to: • Reports or logs from automated mechanisms that perform remediation of VCAs at instantiation; or • Documentation listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R3, Part 3.4

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity documented one or more processes to document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments, including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.
	For each Applicable System, for each assessment conducted according to Parts 3.1, 3.2, and 3.3, verify the results of the assessment were documented.
	For each Applicable System, for each assessment conducted according to Parts 3.1, 3.2, and 3.3, for any vulnerabilities identified, verify: 1. An action plan to remediate or mitigate the identified vulnerabilities was created or modified; 2. the action plan includes a planned date of completion; 3. the action plan includes the execution status of any remediation or mitigation action items; 4. the status of the action plan, if the planned date of completion has been exceeded; and 5. the completion of the action plan, if the action plan status is complete.

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, associated PCA, and associated SCI, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets (TCA) and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for TCAs and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for TCA and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use TCA(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use TCA(s) or Removable Media.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-010-5 R4

This section to be completed by the Compliance Enforcement Authority

Section 1. For TCA(s) managed by the Responsible Entity:	
	Verify that the Responsible Entity has documented at least one plan, as specified in Attachment 1, for TCA(s) that includes: 1. TCA management; 2. TCA authorization; 3. software vulnerability mitigation; 4. introduction of malicious code mitigation; and 5. unauthorized use mitigation.
	Verify that the Responsible Entity has implemented its plan(s) to manage TCA(s) individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.
	For each individual or group of TCA(s), verify the Responsible Entity authorizes: 1. Users, either individually or by group or role; 2. Locations, either individually or by group; and 3. Uses, which shall be limited to what is necessary to perform business functions.
	Verify that the Responsible Entity has implemented one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability): • Security patching, including manual or managed updates; • System hardening; or • Other method(s) to mitigate software vulnerabilities. If a TCA is not fully capable of any of the methods above, then verify the TCA capabilities and the implementation of those capabilities up to the requirement.
	Verify that the Responsible Entity has implemented one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per TCA capability): • Live operating system and software executable only from read-only media; • Antivirus software, including manual or managed updates of signatures or patterns; • Application whitelisting; or • Other method(s) to mitigate the introduction of malicious code. If a TCA is not fully capable of any of the methods above, then verify the TCA capabilities and the implementation of those capabilities up to the requirement.
	Verify that the Responsible Entity has implemented one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s): • Restrict physical access; • Full-disk encryption with authentication; • Multi-factor authentication; or • Other method(s) to mitigate the risk of unauthorized use.

Section 2. For TCA(s) managed by a party other than the Responsible Entity:	
	Verify that the Responsible Entity has documented at least one plan, as specified in Attachment 1, for TCA(s) managed by a party other than the Responsible Entity that includes: 1. Software vulnerability mitigation; 2. introduction of malicious code mitigation; and 3. determination of additional mitigation actions, as necessary.
	Verify that the Responsible Entity has implemented one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability): • Review of installed security patch(es); • review of security patching process used by the party; • review of other vulnerability mitigation performed by the party; or • other method(s) to mitigate software vulnerabilities. If a TCA is not fully capable of any of the methods above, then verify the TCA capabilities and the implementation of those capabilities up to the requirement.
	Verify that the Responsible Entity has implemented one or a combination of the following methods to achieve the objective of mitigating malicious code (per TCA capability): • Review of antivirus update level; • review of antivirus update process used by the party; • review of application whitelisting used by the party; • review use of live operating system and software executable only from read-only media; • review of system hardening used by the party; or • Review of other method(s) to mitigate the risk of introduction of malicious code. If a TCA is not fully capable of any of the methods above, then verify the TCA capabilities and the implementation of those capabilities up to the requirement.
	For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2: 1. Verify that the Responsible Entity determined whether any additional mitigation actions are necessary. 2. If any additional mitigation actions were necessary, verify that such actions were implemented prior to connecting the TCA.

Section 3. For Removable Media:	
	Verify that the Responsible Entity has documented at least one plan, as specified in Attachment 1, for Removable Media that includes: 1. Removable Media authorization; and 2. malicious code mitigation.
	Verify the Responsible Entity authorized, for each individual or group of Removable Media: 1. Users, either individually or by group or role; and 2. locations, either individually or by group.
	Verify the Responsible Entity has implemented method(s) to detect malicious code on Removable Media prior to connecting and mitigated the threat of detected malicious code.

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-010-5 may be found on the NERC Web Site (www.nerc.com) under “Program Areas & Departments”, “Reliability Standards.”

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

CIP-010-5 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets (TCA) and Removable Media as required under Requirement R4.

Section 1. TCA(s) Managed by the Responsible Entity.

1.1. TCA Management: Responsible Entities shall manage TCA(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection, or (3) a combination of both (1) and (2) above.

1.2. TCA Authorization: For each individual or group of TCA(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Security patching, including manual or managed updates;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting;
- Live operating system and software executable only from read only media;
- System hardening; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of TCA(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or

- Other method(s) to mitigate the risk of unauthorized use.

Section 2. TCA(s) Managed by a Party Other than the Responsible Entity.

2.1 Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the TCA (per TCA capability):

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review use of live operating system and software executable only from read only media;
- Review of other vulnerability mitigation performed by the party; or
- Review of other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of introduction of malicious code (per TCA capability):

- Review of antivirus update level;
- Review of antivirus update process used by the party;
- Review of application whitelisting used by the party;
- Review of system hardening used by the party; or
- Review of other method(s) to mitigate the risk of introduction of malicious code.

2.3 For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the TCA.

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media prior to connecting; and

3.2.2. Mitigate the threat of detected malicious code.

CIP-010-5 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the TCA(s). This can be included as part of the TCA plan(s), part of the documentation related to authorization of TCA(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of TCA(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate the risk of software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating system and software executable only from read only media, the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution, system hardening practices or other method(s) to mitigate the risk of software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, methods to maintain the known good state of the OS and all software, or system hardening practices. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the TCA does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that document a review of the use of live operating system and software executable only from read only media; memoranda, electronic mail, policies, or contracts from parties other than the Responsible Entity that document a review of the use of controls that maintain the state of the operating system and software such that it is in a known state prior to execution; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, and system hardening by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for TCA(s) managed by a party other than the Responsible Entity. If a TCA does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the TCA does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the TCA managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on- demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on

Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFTv1	02/28/2024		Initial Draft

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-011-4 – Cyber Security – Information Protection

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		

***** CIP-011-3 is only applicable to DPs that own certain UFLS, UVLS, RAS, Protection Systems, or Cranking Paths. See CIP-011-3 Section 4, Applicability, for details.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

---

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders, and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall implement one or more documented information protection program(s) for BCSI pertaining to Applicable Systems identified in *CIP-01104 Table R1 – Information Protection Program* that collectively includes each of the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-4 Table R1 – Information Protection Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R1 Part 1.1

CIP-011-4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Physical Access Control Systems (PACS) Medium impact BCS and their associated: 1. EACMS; and 2. PACS Shared Cyber Infrastructure (SCI) supporting an Applicable System in this Part	Method(s) to identify BCSI.	Examples of evidence may include, but are not limited to, the following: • Documented method(s) to identify BCSI from the entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BCSI as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BCSI; or • Storage locations identified for housing BCSI in the entity's information protection program.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-011-4, R1, Part 1.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more information protection programs that have method(s) to identify BCSI.
	Verify the Responsible Entity has implemented the method(s) to identify BCSI.

Auditor Notes:

R1 Part 1.2

CIP-011-4 Table R1 – Information Protection Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High impact BCS and their associated: 1. EACMS; and 2. PACS Medium impact BCS and their associated: 1. EACMS; and 2. PACS SCI supporting an Applicable System in this Part	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	Examples of evidence for on-premise BCSI may include, but are not limited to, the following: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BCSI; or • Records indicating that BCSI is handled in a manner consistent with the entity's documented procedure(s). Examples of evidence for off-premise BCSI may include, but are not limited to, the following: • Implementation of electronic technical method(s) to protect electronic BCSI (e.g., data masking, encryption, hashing, tokenization, cipher, electronic key management); or • Implementation of physical technical method(s) to protect physical BCSI (e.g., physical lock and key management, physical badge management, biometrics, alarm system); or • Implementation of administrative method(s) to protect BCSI (e.g., vendor service risk assessments, business agreements).

Registered Entity Response (Required):
Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-011-4, R1, Part 1.2

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more information protection programs that include method(s) for protecting and securely handling BCSI to mitigate risks of compromising confidentiality.
	Verify the Responsible Entity has implemented the methods(s) for protecting and securely handling BCSI to mitigate risks of compromising confidentiality, including storage, transit, and use.

Notes to Auditor:

Authorization of access to BCSI that pertains to BCS, EACMS, and PACS at the medium-without-ERC impact rating should be addressed in the information protection program.

CIP-004-7 R6 applies to provisioned access to BCSI. Other forms of access, if any, should be addressed by the information protection program.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in *CIP-011-4 Table R2 – Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-4 Table R2 – Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-011-4 Table R2 –Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Methods to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).	Examples of evidence may include, but are not limited to, the following: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BCSI such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter (PSP) or other methods used to prevent unauthorized retrieval of BCSI.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed **(This section to be completed by the Compliance Enforcement Authority)**:

Compliance Assessment Approach Specific to CIP-011-4, R2, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has documented one or more processes that have methods to take action to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).
	Verify the Responsible Entity has implemented the method(s) to prevent the unauthorized retrieval of BCSI from Applicable Systems containing BCSI, prior to their disposal or reuse (except for reuse within other systems identified in the Applicable Systems column).

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-011-4 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFTv1	02/28/2024		Initial Draft

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-013-3 – Cyber Security – Supply Chain Risk Management

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Name of Registered Entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements

	BA	DP	GO	GOP	PA/PC	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	*	X	X		X			X	X		
R2	X	*	X	X		X			X	X		
R3	X	*	X	X		X			X	X		

*CIP-013-2 is only applicable to DPs that own certain UFLS, UVLS, RAS, protection systems, or cranking paths. See CIP-013-2 Section 4, Applicability, for details.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

---

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest version of the Reliability Standards, approved by the applicable governmental authority, relevant to its registration status.

The RSAW may provide a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserve the right to request from the registered entity additional evidence that is not included in this RSAW. Additionally, this RSAW may include excerpts from FERC Orders and other regulatory references. The FERC Order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC Orders and the language included in this document, FERC Orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
R3			

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BCS and their associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Shared Cyber infrastructure (SCI). The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of applicable systems listed in Requirement R1 to identify and assess cyber security risk(s) to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring applicable systems listed in Requirement R1 that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor; and

1.2.6. Coordination of controls for vendor-initiated remote access.

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-013-3 R1

This section to be completed by the Compliance Enforcement Authority

	[R1] Verify the Responsible Entity has documented one or more plans to manage the cyber security risk in its supply chain for high and medium impact BCS and their associated EACMS, PACS, and SCI.
	[Part 1.1] Verify the plans collectively contain one or more processes used in planning for the procurement of applicable systems listed in Requirement R1. Verify these processes collectively will result in the identification and assessment of cyber security risks to the BES from vendor products and services resulting from: i. procuring and installing vendor equipment and software; and ii. transitions from one vendor or set of vendors to another vendor or set of vendors.
	[Part 1.2] Verify the plans collectively contain one or more processes used in procurement of applicable systems listed in Requirement R1, and that these processes address the areas identified in Part 1.2.1 through Part 1.2.6. If any of the areas identified in Part 1.2.1 through Part 1.2.6 are not applicable, verify the entity has documented the reason it is not applicable.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium][Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

Registered Entity Response (Required):
Compliance Narrative:
Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-013-3 R2
This section to be completed by the Compliance Enforcement Authority

	For procurements of applicable systems listed in Requirement R1 that begun on or after the effective date of CIP-013-1, verify the Responsible Entity has implemented its documented supply chain cyber security risk management plans specified in Requirement R1.
	For procurements of applicable systems listed in Requirement R1, verify the Responsible Entity has implemented its documented supply chain cyber security risk management plans specified in Requirement R1.
	Note to Auditor: Procurements of medium or high impact BCS began on or after the effective date of CIP-013-1.

	Procurements of EACMS and PACS began on or after the effective date of CIP-013-2. Procurements of SCI began on or after the effective date of CIP-013-3.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.

File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-013-3 R3

This section to be completed by the Compliance Enforcement Authority

	Verify the Responsible Entity has reviewed its supply chain cyber security risk management plans specified in Requirement R1 on or before the effective date of CIP-013-1, and at least once every 15 calendar months thereafter.
	Verify the Responsible Entity has obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plans specified in Requirement R1 on or before the effective date of CIP-013-1, and at least once every 15 calendar months thereafter.

Auditor Notes:

____

Additional Information:

Reliability Standard

The full text of CIP-013-3may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Standards", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language

See FERC Order 822

Revision History for RSAW

Version	Date	Reviewers	Revision Description
DRAFTv1	02/28/2024		Initial Draft

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standards Announcement

Project 2016-02 Modifications to CIP Standards | Virtualization

Final Ballots Open through April 12, 2024

Now Available

Final ballots for the **CIP Virtualization suite of standards (outlined below)** are open through **8 p.m. Eastern, Friday, April 12, 2024.**

- CIP-002-7 - Cyber Security – BES Cyber System Categorization
- CIP-003-10 - Cyber Security – Security Management Controls
- CIP-004-8 - Cyber Security – Personnel & Training
- CIP-005-8 - Cyber Security – BES Cyber System Logical Isolation
- CIP-006-7 - Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-7 - Cyber Security – Systems Security Management
- CIP-008-7 - Cyber Security – Incident Reporting and Response Planning
- CIP-009-7 - Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-5 - Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-4 - Cyber Security – Information Protection
- CIP-013-3 - Cyber Security – Supply Chain Risk Management

Balloting

In the final ballot, votes are counted by exception. Votes from the previous ballot are automatically carried over in the final ballot. Only members of the applicable ballot pools can cast a vote. Ballot pool members who previously voted have the option to change their vote in the final ballot. Ballot pool members who did not cast a vote during the previous ballot can vote in the final ballot.

Members of the ballot pool(s) associated with this project can log into the Standards Balloting and Commenting System (SBS) and submit votes here.

- *Contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern) for problems regarding accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out.*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*

- *Please be mindful of ballot and comment period closing dates. We ask to* ***allow at least 48 hours*** *for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts* ***prior to the last day*** *of a comment/ballot period.*

Next Steps

The voting results will be posted and announced after the ballots close. If approved, the standards will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

For information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Manager of Standards Development, Alison Oswald (via email) or at (404) 446-9410.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-002-7 FN 5 ST
Voting Start Date: 4/3/2024 11:54:11 AM
Voting End Date: 4/12/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 5
Total # Votes: 253
Total Ballot Pool: 299
Quorum: 84.62
Quorum Established Date: 4/3/2024 4:18:00 PM
Weighted Segment Value: 94.37

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	63	0.94	4	0.06	0	5	14
Segment: 2	8	0.6	5	0.5	1	0.1	0	1	1
Segment: 3	66	1	52	0.963	2	0.037	0	3	9
Segment: 4	15	1	11	1	0	0	0	2	2
Segment: 5	71	1	51	0.944	3	0.056	0	4	13
Segment: 6	44	1	32	0.914	3	0.086	0	2	7
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.4	4	0.4	0	0	0	3	0
Totals:	299	6	218	5.662	13	0.338	0	22	46

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Matt Lewis		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Negative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Abstain	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	N/A
1	New York Power Authority	Daniel Valle		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		None	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Negative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Salt River Project	Thomas Johnson		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		Negative	N/A
6	Imperial Irrigation District	Diana Torres		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Kelly Bertholet		Negative	N/A
6	Muscatine Power and Water	Nicholas Burns		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	New York State Reliability Council	Wesley Yeomans		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 299 of 299 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-003-9 FN 6 ST
Voting Start Date: 4/3/2024 11:55:02 AM
Voting End Date: 4/12/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 6
Total # Votes: 255
Total Ballot Pool: 298
Quorum: 85.57
Quorum Established Date: 4/3/2024 4:18:12 PM
Weighted Segment Value: 93.63

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	61	0.91	6	0.09	0	7	12
Segment: 2	8	0.5	5	0.5	0	0	0	1	2
Segment: 3	65	1	48	0.941	3	0.059	0	5	9
Segment: 4	15	1	9	0.9	1	0.1	0	3	2
Segment: 5	71	1	48	0.923	4	0.077	0	7	12
Segment: 6	44	1	33	0.943	2	0.057	0	4	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.5	5	0.5	0	0	0	1	1
Totals:	298	6	209	5.618	16	0.382	0	30	43

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Micah Runner		Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	N/A
1	New York Power Authority	Daniel Valle		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Abstain	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Affirmative	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Josh Combs		Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Abstain	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Adam Lee		None	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Sheila Suurmeier		Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Negative	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	N/A
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Affirmative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	N/A
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Rachel Schuldt		Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Imperial Irrigation District	Diana Torres	Denise Sanchez	Abstain	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Affirmative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 298 of 298 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-004-7 FN 6 ST
Voting Start Date: 4/3/2024 12:03:11 PM
Voting End Date: 4/12/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 6
Total # Votes: 254
Total Ballot Pool: 296
Quorum: 85.81
Quorum Established Date: 4/3/2024 4:19:13 PM
Weighted Segment Value: 86.3

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	56	0.824	12	0.176	0	6	12
Segment: 2	8	0.6	6	0.6	0	0	0	0	2
Segment: 3	65	1	43	0.86	7	0.14	0	6	9
Segment: 4	14	1	8	0.8	2	0.2	0	3	1
Segment: 5	71	1	42	0.824	9	0.176	0	8	12
Segment: 6	43	1	30	0.857	5	0.143	0	3	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.5	5	0.5	0	0	0	1	1
Totals:	296	6.1	190	5.264	35	0.836	0	29	42

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	N/A
1	New York Power Authority	Daniel Valle		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Negative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	N/A
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Negative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Affirmative	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Abstain	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Negative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-005-8 FN 6 ST
Voting Start Date: 4/3/2024 11:56:27 AM
Voting End Date: 4/12/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 6
Total # Votes: 254
Total Ballot Pool: 296
Quorum: 85.81
Quorum Established Date: 4/3/2024 4:18:42 PM
Weighted Segment Value: 75.73

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	50	0.746	17	0.254	0	7	12
Segment: 2	8	0.6	5	0.5	1	0.1	0	0	2
Segment: 3	65	1	39	0.78	11	0.22	0	6	9
Segment: 4	14	0.9	6	0.6	3	0.3	0	4	1
Segment: 5	71	1	38	0.731	14	0.269	0	7	12
Segment: 6	43	1	25	0.735	9	0.265	0	4	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.3	3	0.3	0	0	0	3	1
Totals:	296	5.8	166	4.392	55	1.408	0	33	42

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Negative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Negative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	N/A
1	Georgia Transmission Corporation	Greg Davis		Abstain	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	N/A
1	New York Power Authority	Daniel Valle		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Negative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	N/A
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Negative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Negative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Negative	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Negative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Abstain	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Negative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Negative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Negative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Abstain	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Quincy Wang		Negative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Negative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Negative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Negative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Negative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Negative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Negative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Negative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Negative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Tyler Schwendiman		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-006-7 FN 5 ST
Voting Start Date: 4/3/2024 11:57:09 AM
Voting End Date: 4/12/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 5
Total # Votes: 249
Total Ballot Pool: 297
Quorum: 83.84
Quorum Established Date: 4/3/2024 4:18:53 PM
Weighted Segment Value: 94.7

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	63	0.955	3	0.045	0	5	15
Segment: 2	8	0.6	5	0.5	1	0.1	0	1	1
Segment: 3	66	1	51	0.944	3	0.056	0	3	9
Segment: 4	14	1	11	1	0	0	0	2	1
Segment: 5	71	1	50	0.943	3	0.057	0	4	14
Segment: 6	43	1	31	0.939	2	0.061	0	2	8
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.4	4	0.4	0	0	0	3	0
Totals:	297	6	215	5.682	12	0.318	0	22	48

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Matt Lewis		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Abstain	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Daniel Valle		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Negative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Affirmative	N/A
3	Portland General Electric Co.	Mayra Franco		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Tyler Schwendiman		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Showing 1 to 297 of 297 entries

Previous 1 Next

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-007-7 FN 6 ST
Voting Start Date: 4/3/2024 11:58:49 AM
Voting End Date: 4/12/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 6
Total # Votes: 254
Total Ballot Pool: 296
Quorum: 85.81
Quorum Established Date: 4/3/2024 4:19:02 PM
Weighted Segment Value: 90.24

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	60	0.882	8	0.118	0	6	12
Segment: 2	8	0.6	5	0.5	1	0.1	0	0	2
Segment: 3	65	1	45	0.918	4	0.082	0	7	9
Segment: 4	14	0.9	8	0.8	1	0.1	0	4	1
Segment: 5	71	1	46	0.902	5	0.098	0	8	12
Segment: 6	43	1	31	0.912	3	0.088	0	4	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.5	5	0.5	0	0	0	1	1
Totals:	296	6	200	5.414	22	0.586	0	32	42

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	N/A
1	New York Power Authority	Daniel Valle		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Negative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Affirmative	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Abstain	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Affirmative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Abstain	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Affirmative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		None	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Tyler Schwendiman		Affirmative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Affirmative	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 296 of 296 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-008-7 FN 5 ST
Voting Start Date: 4/3/2024 12:04:36 PM
Voting End Date: 4/12/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 5
Total # Votes: 249
Total Ballot Pool: 297
Quorum: 83.84
Quorum Established Date: 4/3/2024 4:19:23 PM
Weighted Segment Value: 96.05

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	64	0.97	2	0.03	0	5	15
Segment: 2	8	0.6	5	0.5	1	0.1	0	1	1
Segment: 3	66	1	51	0.962	2	0.038	0	4	9
Segment: 4	14	1	11	1	0	0	0	2	1
Segment: 5	71	1	50	0.962	2	0.038	0	5	14
Segment: 6	43	1	32	0.97	1	0.03	0	2	8
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.4	4	0.4	0	0	0	3	0
Totals:	297	6	217	5.763	8	0.237	0	24	48

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Matt Lewis		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Abstain	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Daniel Valle		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Tyler Schwendiman		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Showing 1 to 297 of 297 entries

Previous 1 Next

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-009-7 FN 5 ST
Voting Start Date: 4/3/2024 12:07:03 PM
Voting End Date: 4/12/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 5
Total # Votes: 249
Total Ballot Pool: 297
Quorum: 83.84
Quorum Established Date: 4/3/2024 4:19:36 PM
Weighted Segment Value: 95.8

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	63	0.955	3	0.045	0	5	15
Segment: 2	8	0.6	5	0.5	1	0.1	0	1	1
Segment: 3	66	1	51	0.962	2	0.038	0	4	9
Segment: 4	14	1	11	1	0	0	0	2	1
Segment: 5	71	1	50	0.962	2	0.038	0	5	14
Segment: 6	43	1	32	0.97	1	0.03	0	2	8
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.4	4	0.4	0	0	0	3	0
Totals:	297	6	216	5.748	9	0.252	0	24	48

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Matt Lewis		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Abstain	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	N/A
1	New York Power Authority	Daniel Valle		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Affirmative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	National Grid USA	Robin Berry		Affirmative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Affirmative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Tyler Schwendiman		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 297 of 297 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-010-5 FN 6 ST
Voting Start Date: 4/3/2024 12:07:44 PM
Voting End Date: 4/12/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 6
Total # Votes: 255
Total Ballot Pool: 296
Quorum: 86.15
Quorum Established Date: 4/3/2024 4:19:46 PM
Weighted Segment Value: 76.98

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	54	0.794	14	0.206	0	6	12
Segment: 2	8	0.6	2	0.2	4	0.4	0	0	2
Segment: 3	65	1	41	0.837	8	0.163	0	7	9
Segment: 4	14	0.9	8	0.8	1	0.1	0	4	1
Segment: 5	71	1	39	0.765	12	0.235	0	8	12
Segment: 6	43	1	28	0.824	6	0.176	0	4	5
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.5	4	0.4	1	0.1	0	2	0
Totals:	296	6	176	4.619	46	1.381	0	33	41

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Abstain	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		Affirmative	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Negative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Negative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	Affirmative	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		Affirmative	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		None	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Negative	N/A
1	Entergy	Brian Lindsey		Negative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	None	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		None	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte		Negative	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	Abstain	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Abstain	N/A
1	Lower Colorado River Authority	Matt Lewis	James Baldwin	Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Affirmative	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Negative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	N/A
1	New York Power Authority	Daniel Valle		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Negative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		None	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Negative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		None	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Negative	N/A
1	Salt River Project	Sarah Blankenship	Israel Perez	Negative	N/A
1	SaskPower	Wayne Guttormson		Affirmative	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Wabash Valley Power Association	Joni Jones		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Negative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Affirmative	N/A
2	Independent Electricity System Operator	Helen Lainis		None	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		None	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Negative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips	Shannon Mickens	Negative	N/A
3	AEP	Leshel Hutchings		None	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	Affirmative	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez	Ellese Murphy	Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		None	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner	Denise Sanchez	Abstain	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A
3	Lakeland Electric	Steven Marshall		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		Abstain	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Negative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Negative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		None	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		None	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Negative	N/A
3	Salt River Project	Mathew Weber	Israel Perez	Negative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		None	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		Abstain	N/A
3	WEC Energy Group, Inc.	Christine Kane		Abstain	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Abstain	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Negative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss	Candace Morakinyo	Abstain	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Abstain	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Quincy Wang		Negative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	Affirmative	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Michelle Pagano		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		None	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Negative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		Negative	N/A
5	Imperial Irrigation District	Tino Zaragoza	Denise Sanchez	Abstain	N/A
5	Lakeland Electric	Carmen Rodriguez		Affirmative	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		Abstain	N/A
5	Lower Colorado River Authority	Teresa Krabe		Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		None	N/A
5	Muscatine Power and Water	Neal Nelson		Affirmative	N/A
5	National Grid USA	Robin Berry		Negative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Negative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Abstain	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	N/A
5	Orlando Utilities Commission	Dania Colon		None	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Negative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		None	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Negative	N/A
5	Salt River Project	Thomas Johnson	Israel Perez	Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Affirmative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		Affirmative	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		None	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Abstain	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	Affirmative	N/A
6	Bonneville Power Administration	Tanner Brier		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Tiffany Lake	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		None	N/A
6	Lakeland Electric	Paul Shipps		Affirmative	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Abstain	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Affirmative	N/A
6	New York Power Authority	Shelly Dineen		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Negative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Negative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		None	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Negative	N/A
6	Salt River Project	Timothy Singh	Israel Perez	Negative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Abstain	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		Affirmative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Tyler Schwendiman		Negative	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Showing 1 to 296 of 296 entries

Previous 1 Next

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-011-3 FN 5 ST
Voting Start Date: 4/3/2024 12:09:28 PM
Voting End Date: 4/12/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 5
Total # Votes: 249
Total Ballot Pool: 297
Quorum: 83.84
Quorum Established Date: 4/3/2024 4:19:58 PM
Weighted Segment Value: 86.21

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	61	0.924	5	0.076	0	5	15
Segment: 2	8	0.6	2	0.2	4	0.4	0	1	1
Segment: 3	66	1	49	0.925	4	0.075	0	4	9
Segment: 4	14	1	11	1	0	0	0	2	1
Segment: 5	71	1	46	0.885	6	0.115	0	5	14
Segment: 6	43	1	31	0.939	2	0.061	0	2	8
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	297	6	203	5.173	22	0.827	0	24	48

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Matt Lewis		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Abstain	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Negative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Negative	N/A
1	New York Power Authority	Daniel Valle		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		Negative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Negative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Negative	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	National Grid USA	Robin Berry		Negative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		Negative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Tyler Schwendiman		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Showing 1 to 297 of 297 entries

BALLOT RESULTS

Ballot Name: 2016-02 Modifications to CIP Standards | Virtualization CIP-013-3 FN 5 ST
Voting Start Date: 4/3/2024 12:12:06 PM
Voting End Date: 4/12/2024 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 5
Total # Votes: 249
Total Ballot Pool: 297
Quorum: 83.84
Quorum Established Date: 4/3/2024 4:20:10 PM
Weighted Segment Value: 86.47

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	86	1	62	0.939	4	0.061	0	5	15
Segment: 2	8	0.6	2	0.2	4	0.4	0	1	1
Segment: 3	66	1	49	0.925	4	0.075	0	4	9
Segment: 4	14	1	11	1	0	0	0	2	1
Segment: 5	71	1	46	0.885	6	0.115	0	5	14
Segment: 6	43	1	31	0.939	2	0.061	0	2	8
Segment: 7	1	0	0	0	0	0	0	1	0
Segment: 8	1	0	0	0	0	0	0	1	0
Segment: 9	0	0	0	0	0	0	0	0	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 10	7	0.4	3	0.3	1	0.1	0	3	0
Totals:	297	6	204	5.188	21	0.812	0	24	48

BALLOT POOL MEMBERS

Show All entries

Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Ameren - Ameren Services	Tamara Evey		Affirmative	N/A
1	American Transmission Company, LLC	Amy Wilke		None	N/A
1	APS - Arizona Public Service Co.	Daniela Atanasovski		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	Jennifer Bray		Affirmative	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		Affirmative	N/A
1	Avista - Avista Corporation	Mike Magruder		Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Tim Kelley	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Adrian Andreoiu		Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		Affirmative	N/A
1	Black Hills Corporation	Seth Nelson	Jennifer Malon	None	N/A
1	Bonneville Power Administration	Kamala Rogers-Holliday		Affirmative	N/A
1	CenterPoint Energy Houston Electric, LLC	Daniela Hammons		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		Affirmative	N/A
1	Central Hudson Gas & Electric Corp.	Michael Ridolfino		None	N/A
1	City Utilities of Springfield, Missouri	Michael Bowman		Affirmative	N/A
1	Cleco Corporation	John Lindsey	Clay Walker	Affirmative	N/A
1	Colorado Springs Utilities	Corey Walker		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Karrie Schuldt		Affirmative	N/A
1	Dominion - Dominion Virginia Power	Elizabeth Weber		Affirmative	N/A
1	Duke Energy	Katherine Street		Affirmative	N/A
1	East Kentucky Power Cooperative	Amber Skillern		Abstain	N/A
1	Entergy	Brian Lindsey		Affirmative	N/A
1	Evergy	Kevin Frick	Alan Kloster	Affirmative	N/A
1	Eversource Energy	Joshua London		Affirmative	N/A
1	Exelon	Daniel Gacek		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
1	Georgia Transmission Corporation	Greg Davis		Affirmative	N/A
1	Glencoe Light and Power Commission	Terry Volkmann		Negative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh	Mark Ciufo	Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	N/A
1	Hydro-Quebec (HQ)	Nicolas Turcotte	Chantal Mazza	None	N/A
1	IDACORP - Idaho Power Company	Sean Steffensen		None	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz	Denise Sanchez	None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Gail Elliott	Affirmative	N/A
1	KAMO Electric Cooperative	Micah Breedlove		Affirmative	N/A
1	Lakeland Electric	Larry Watt		None	N/A
1	Lincoln Electric System	Josh Johnson		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Matt Lewis		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Nazra Gladu		Affirmative	N/A
1	MEAG Power	David Weekley	John Daho	Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard	Andy Fuhrman	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andrew Kurriger		Abstain	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Negative	N/A
1	NB Power Corporation	Jeffrey Streifling		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Affirmative	N/A
1	Network and Security Technologies	Nick Lauriat	Roger Fradenburgh	Affirmative	N/A
1	New York Power Authority	Daniel Valle		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
1	NiSource - Northern Indiana Public Service Co.	Alison Nickells		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Brett Douglas		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Oncor Electric Delivery	Byron Booker		Affirmative	N/A
1	Orlando Utilities Commission	Aaron Staley		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Pacific Gas and Electric Company	Marco Rios	Michael Johnson	Affirmative	N/A
1	Portland General Electric Co.	Brooke Jockin		Affirmative	N/A
1	PPL Electric Utilities Corporation	Michelle McCartney Longo		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Karen Arnold		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Chelan County	Diane E Landry		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Alyssia Rhoads		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Joanne Anderson		Affirmative	N/A
1	Sacramento Municipal Utility District	Wei Shao	Tim Kelley	Affirmative	N/A
1	Salt River Project	Matthew Jaramilla	Israel Perez	Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	Seattle City Light	Michael Jang		Abstain	N/A
1	Seminole Electric Cooperative, Inc.	Kristine Ward		None	N/A
1	Sempra - San Diego Gas and Electric	Mohamed Derbas		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Matt Carden		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Abstain	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell	Jennie Wike	Affirmative	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Abstain	N/A
1	Tennessee Valley Authority	David Plumb		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Donna Wood		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		None	N/A
1	Wabash Valley Power Association	Joni Jones		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	Ben Hammer		Affirmative	N/A
1	Xcel Energy, Inc.	Eric Barry		Affirmative	N/A
2	California ISO	Darcy O'Connell		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Kennedy Meier		Abstain	N/A
2	Independent Electricity System Operator	Helen Lainis		Negative	N/A
2	ISO New England, Inc.	Michael Puscas	John Galloway	Negative	N/A
2	Midcontinent ISO, Inc.	Bobbi Welch		Affirmative	N/A
2	New York Independent System Operator	Gregory Campoli		Negative	N/A
2	PJM Interconnection, L.L.C.	Thomas Foster	Elizabeth Davis	Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Joshua Phillips		None	N/A
3	AEP	Leshel Hutchings		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras Sr		Affirmative	N/A
3	APS - Arizona Public Service Co.	Jessica Lopez		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	Lovita Griffin		Affirmative	N/A
3	Avista - Avista Corporation	Robert Follini		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Joseph Amato		Affirmative	N/A
3	Black Hills Corporation	Don Stahl	Jennifer Malon	None	N/A
3	Bonneville Power Administration	Ron Sporseen		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City Utilities of Springfield, Missouri	Jessica Morrissey		Affirmative	N/A
3	Cleco Corporation	Maurice Paulk	Clay Walker	Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		None	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Dominion - Dominion Virginia Power	Bill Garvey		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Marvin Johnson		Affirmative	N/A
3	Duke Energy - Florida Power Corporation	Marcelo Pesantez		Affirmative	N/A
3	East Kentucky Power Cooperative	Chris Adams		None	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	Evergy	Marcus Moor	Alan Kloster	Affirmative	N/A
3	Eversource Energy	Vicki O'Leary		Affirmative	N/A
3	Exelon	Kinte Whitehead		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Negative	N/A
3	Great River Energy	Michael Brytowski		Affirmative	N/A
3	Hydro One Networks, Inc.	Paul Malozewski		Affirmative	N/A
3	Imperial Irrigation District	George Kirschner		Affirmative	N/A
3	KAMO Electric Cooperative	Tony Gott		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	Steven Marshall		None	N/A
3	Lincoln Electric System	Sam Christensen		Affirmative	N/A
3	Los Angeles Department of Water and Power	Fausto Serratos		None	N/A
3	M and A Electric Power Cooperative	Gary Dollins		Affirmative	N/A
3	MEAG Power	Roger Brand	John Daho	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Abstain	N/A
3	National Grid USA	Brian Shanahan		Negative	N/A
3	Nebraska Public Power District	Tony Eddleman		Affirmative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Steven Taddeucci		Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	Northern California Power Agency	Michael Whitney	Chris Carnesi	Negative	N/A
3	NW Electric Power Cooperative, Inc.	Heath Henry		Affirmative	N/A
3	Ocala Utility Services	Neville Bowen	LaKenya Vannorman	None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	David Heins		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		Affirmative	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		None	N/A
3	Owensboro Municipal Utilities	William Berry		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Pacific Gas and Electric Company	Sandra Ellis	Michael Johnson	Affirmative	N/A
3	Platte River Power Authority	Richard Kiess		Abstain	N/A
3	Portland General Electric Co.	Mayra Franco		Affirmative	N/A
3	PPL - Louisville Gas and Electric Co.	James Frank		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Sacramento Municipal Utility District	Nicole Looney	Tim Kelley	Affirmative	N/A
3	Salt River Project	Mathew Weber		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	Marc Sedor		Abstain	N/A
3	Sempra - San Diego Gas and Electric	Bryan Bennett		Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jarrod Murdaugh		Affirmative	N/A
3	Snohomish County PUD No. 1	Holly Chaney		Affirmative	N/A
3	Southern Company - Alabama Power Company	Joel Dembowski		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Ryan Snyder		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	John Nierenberg		None	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Unitil	Paul Krell		None	N/A
3	WEC Energy Group, Inc.	Christine Kane		Affirmative	N/A
3	Xcel Energy, Inc.	Nicholas Friebel		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	City Utilities of Springfield, Missouri	Jerry Bradshaw		Affirmative	N/A
4	CMS Energy - Consumers Energy Company	Aric Root		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Mark Garza		Affirmative	N/A
4	Georgia System Operations Corporation	Katrina Lyons		Affirmative	N/A
4	LaGen	Wayne Messina	Clay Walker	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John D. Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Karla Weaver		Abstain	N/A
4	Sacramento Municipal Utility District	Foung Mua	Tim Kelley	Affirmative	N/A
4	Seattle City Light	Robert Jones		None	N/A
4	Seminole Electric Cooperative, Inc.	Ken Habgood		Abstain	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho	Jennie Wike	Affirmative	N/A
4	Utility Services, Inc.	Carver Powers		Affirmative	N/A
4	WEC Energy Group, Inc.	Matthew Beilfuss		Affirmative	N/A
5	Acciona Energy North America	Truong Le		None	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		None	N/A
5	APS - Arizona Public Service Co.	Andrew Smith		Affirmative	N/A
5	Associated Electric Cooperative, Inc.	Chuck Booth		Affirmative	N/A
5	Austin Energy	Michael Dillard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	BC Hydro and Power Authority	Quincy Wang		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Dwanique Spiller		Affirmative	N/A
5	Black Hills Corporation	Derek Silbaugh	Jennifer Malon	None	N/A
5	Bonneville Power Administration	Juergen Bermejo		Affirmative	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		Affirmative	N/A
5	Cleco Corporation	Stephanie Huffman	Clay Walker	Affirmative	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Cogentrix Energy Power Management, LLC	Gerry Adamski		None	N/A
5	Colorado Springs Utilities	Jeffrey Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Helen Wang		Affirmative	N/A
5	Constellation	Alison MacKellar		Affirmative	N/A
5	Cowlitz County PUD	Deanna Carlson		Abstain	N/A
5	Dairyland Power Cooperative	Tommy Drea		Affirmative	N/A
5	Dominion - Dominion Resources, Inc.	Anna Salmon		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Mohamad Elhusseini		Affirmative	N/A
5	Duke Energy	Dale Goodwine		Affirmative	N/A
5	East Kentucky Power Cooperative	Davidw Meade		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Selene Willis		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		None	N/A
5	Entergy - Entergy Services, Inc.	Gail Golden		Affirmative	N/A
5	Evergy	Jeremy Harris	Alan Kloster	Affirmative	N/A
5	FirstEnergy - FirstEnergy Corporation	Matthew Augustin		Affirmative	N/A
5	Hydro-Quebec (HQ)	Junji Yamaguchi		None	N/A
5	Imperial Irrigation District	Tino Zaragoza		Affirmative	N/A
5	Lakeland Electric	Carmen Rodriguez		None	N/A
5	Lincoln Electric System	Brittany Millard		Affirmative	N/A
5	Los Angeles Department of Water and Power	Glenn Barry		None	N/A
5	Lower Colorado River Authority	Teresa Krabe	Wesley Maurer	Affirmative	N/A
5	Manitoba Hydro	Kristy-Lee Young		None	N/A
5	Massachusetts Municipal Wholesale Electric Company	Michael Russell		Negative	N/A
5	Muscatine Power and Water	Neal Nelson		Abstain	N/A
5	National Grid USA	Robin Berry		Negative	N/A
5	NB Power Corporation - New Brunswick Power Transmission Corporation	Fon Hiew		Abstain	N/A
5	Nebraska Public Power District	Ronald Bender		Affirmative	N/A
5	New York Power Authority	Zahid Qayyum		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NiSource - Northern Indiana Public Service Co.	Kathryn Tackett		Affirmative	N/A
5	Northern California Power Agency	Jeremy Lawson	Chris Carnesi	Negative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Affirmative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	Patrick Wells		Affirmative	N/A
5	Oglethorpe Power Corporation	Donna Johnson		Affirmative	N/A
5	Ontario Power Generation Inc.	Constantin Chitescu		Negative	N/A
5	Orlando Utilities Commission	Dania Colon		Affirmative	N/A
5	OTP - Otter Tail Power Company	Stacy Wahlund		None	N/A
5	Pacific Gas and Electric Company	Ed Hanson	Michael Johnson	Affirmative	N/A
5	Platte River Power Authority	Jon Osell		Abstain	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Julie Hostrander		Affirmative	N/A
5	PSEG Nuclear LLC	Tim Kucey		None	N/A
5	Public Utility District No. 1 of Chelan County	Rebecca Zahler		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Becky Burden		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Nikkee Hebdon		Affirmative	N/A
5	Sacramento Municipal Utility District	Nicole Goi	Tim Kelley	Affirmative	N/A
5	Salt River Project	Thomas Johnson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seminole Electric Cooperative, Inc.	Melanie Wong		Abstain	N/A
5	Sempra - San Diego Gas and Electric	Jennifer Wright		Affirmative	N/A
5	Southern Company - Southern Company Generation	Leslie Burke		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Larry Rogers		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Ozan Ferrin	Jennie Wike	Affirmative	N/A
5	Talen Generation, LLC	Donald Lock		Negative	N/A
5	Tennessee Valley Authority	Darren Boehm		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Kalidass		None	N/A
5	WEC Energy Group, Inc.	Clarice Zellmer		Affirmative	N/A
5	Xcel Energy, Inc.	Gerry Huitt		Affirmative	N/A
6	AEP	Mathew Miller		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Marcus Bortman		Affirmative	N/A
6	Austin Energy	Imane Mrini		Affirmative	N/A
6	Basin Electric Power Cooperative	Eve G Stromer		None	N/A
6	Berkshire Hathaway - PacifiCorp	Lindsay Wickizer		Affirmative	N/A
6	Black Hills Corporation	Brooke Voorhees	Jennifer Malon	None	N/A
6	Bonneville Power Administration	Tanner Brier		None	N/A
6	Cleco Corporation	Robert Hirchak	Clay Walker	Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Jason Chandler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Constellation	Kimberly Turco		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	John Sturgeon		Affirmative	N/A
6	Evergy	Jennifer Flandermeyer	Alan Kloster	Affirmative	N/A
6	FirstEnergy - FirstEnergy Corporation	Stacey Sheehan		Affirmative	N/A
6	Great River Energy	Brian Meloy		Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Manitoba Hydro	Kelly Bertholet		Affirmative	N/A
6	Muscatine Power and Water	Nicholas Burns		Abstain	N/A
6	New York Power Authority	Shelly Dineen		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Justin Welty		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Dmitriy Bazylyuk		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet	Chris Carnesi	Negative	N/A
6	NRG - NRG Energy, Inc.	Martin Sidor		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Ashley F Stringer		Affirmative	N/A
6	Omaha Public Power District	Shonda McCain		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Abstain	N/A
6	Portland General Electric Co.	Stefanie Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Anne Kronshage		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	Mike Stussy		Affirmative	N/A
6	Sacramento Municipal Utility District	Charles Norton	Tim Kelley	Affirmative	N/A
6	Salt River Project	Timothy Singh		Affirmative	N/A
6	Snohomish County PUD No. 1	John Liang		Affirmative	N/A
6	Southern Company - Southern Company Generation	Ron Carlsen		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Kati Barr		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Terry Gifford	Jennie Wike	Affirmative	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		None	N/A
6	Tennessee Valley Authority	Armando Rodriguez		Affirmative	N/A
6	WEC Energy Group, Inc.	David Boeshaar		Affirmative	N/A
6	Xcel Energy, Inc.	Steve Szablya		Affirmative	N/A
7	Amazon Web Services	Maggy Powell		Abstain	N/A
8	Florida Reliability Coordinating Council – Member Services Division	Vince Ordax		Abstain	N/A
10	Midwest Reliability Organization	Mark Flanary		Affirmative	N/A
10	New York State Reliability Council	Wesley Yeomans		Negative	N/A
10	Northeast Power Coordinating Council	Gerry Dunbar		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Tyler Schwendiman		Abstain	N/A
10	SERC Reliability Corporation	Dave Krueger		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 297 of 297 entries

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Exhibit H

Standard Drafting Team Roster

Standard Drafting Team Roster

Project 2016-02 Modifications to CIP Standards

	Name	Entity
Co-Chair	Jay Cribb	Southern Company
Co-Chair	Matthew Hyatt	Tennessee Valley Authority
Members	Jake Brown	ERCOT
	Norman Dang	Independent Electricity System Operator of Ontario
	Scott Klauminzer	Tacoma Public Utilities, Tacoma Power
	Sharon Koller	American Transmission Company, LLC
	Heather Morgan	EDP Renewables
	Mark Riley	AECI
PMOS Liaisons	Kirk Rosener	CPS Energy
	Ruida Shu	NPCC
NERC Staff	Alison Oswald – Manager of Standards Development	North American Electric Reliability Corporation
	Marisa Hecht – Counsel	North American Electric Reliability Corporation